

# CIS Red Hat Enterprise Linux 8 STIG Benchmark

v2.0.0 - 11-25-2024

# Terms of Use

Please see the below link for our current terms of use:

<https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/>

For information on referencing and/or citing CIS Benchmarks in 3<sup>rd</sup> party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal ([CISLegal@cisecurity.org](mailto:CISLegal@cisecurity.org)) and request guidance on copyright usage.

**NOTE:** It is **NEVER** acceptable to host a CIS Benchmark in **ANY** format (PDF, etc.) on a 3<sup>rd</sup> party (non-CIS owned) site.

# Table of Contents

|                                                                          |           |
|--------------------------------------------------------------------------|-----------|
| <b>Terms of Use .....</b>                                                | <b>1</b>  |
| <b>Table of Contents .....</b>                                           | <b>2</b>  |
| <b>Overview .....</b>                                                    | <b>18</b> |
| <b>Important Usage Information .....</b>                                 | <b>18</b> |
| Key Stakeholders .....                                                   | 18        |
| Apply the Correct Version of a Benchmark .....                           | 19        |
| Exceptions .....                                                         | 19        |
| Remediation .....                                                        | 20        |
| Summary .....                                                            | 20        |
| <b>Target Technology Details .....</b>                                   | <b>21</b> |
| <b>Intended Audience.....</b>                                            | <b>21</b> |
| <b>Consensus Guidance .....</b>                                          | <b>22</b> |
| <b>Typographical Conventions.....</b>                                    | <b>23</b> |
| <b>Recommendation Definitions.....</b>                                   | <b>24</b> |
| Title.....                                                               | 24        |
| <b>Assessment Status.....</b>                                            | <b>24</b> |
| Automated .....                                                          | 24        |
| Manual.....                                                              | 24        |
| Profile .....                                                            | 24        |
| Description.....                                                         | 24        |
| Rationale Statement .....                                                | 24        |
| Impact Statement.....                                                    | 25        |
| Audit Procedure.....                                                     | 25        |
| Remediation Procedure.....                                               | 25        |
| Default Value.....                                                       | 25        |
| References .....                                                         | 25        |
| CIS Critical Security Controls® (CIS Controls®) .....                    | 25        |
| Additional Information.....                                              | 25        |
| Profile Definitions .....                                                | 26        |
| Acknowledgements .....                                                   | 27        |
| <b>Recommendations .....</b>                                             | <b>28</b> |
| <b>1 Initial Setup .....</b>                                             | <b>28</b> |
| <b>1.1 Filesystem .....</b>                                              | <b>29</b> |
| <b>1.1.1 Configure Filesystem Kernel Modules.....</b>                    | <b>30</b> |
| 1.1.1.1 Ensure cramfs kernel module is not available (Automated) .....   | 31        |
| 1.1.1.2 Ensure freevxfs kernel module is not available (Automated) ..... | 36        |

|                                                                                                                                           |            |
|-------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 1.1.1.3 Ensure hfs kernel module is not available (Automated)                                                                             | 41         |
| 1.1.1.4 Ensure hfsplus kernel module is not available (Automated)                                                                         | 46         |
| 1.1.1.5 Ensure jffs2 kernel module is not available (Automated)                                                                           | 51         |
| 1.1.1.6 Ensure overlayfs kernel module is not available (Automated)                                                                       | 56         |
| 1.1.1.7 Ensure squashfs kernel module is not available (Automated)                                                                        | 61         |
| 1.1.1.8 Ensure udf kernel module is not available (Automated)                                                                             | 66         |
| 1.1.1.9 Ensure usb-storage kernel module is not available (Automated)                                                                     | 71         |
| 1.1.1.10 Ensure unused filesystems kernel modules are not available (Manual)                                                              | 76         |
| 1.1.1.11 Ensure the operating system disables the ability to load the firewire-core kernel module (Automated)                             | 82         |
| 1.1.1.12 Ensure a camera is not installed (Automated)                                                                                     | 84         |
| <b>1.1.2 Configure Filesystem Partitions</b>                                                                                              | <b>87</b>  |
| <b>1.1.2.1 Configure /tmp</b>                                                                                                             | <b>88</b>  |
| 1.1.2.1.1 Ensure /tmp is a separate partition (Automated)                                                                                 | 89         |
| 1.1.2.1.2 Ensure nodev option set on /tmp partition (Automated)                                                                           | 93         |
| 1.1.2.1.3 Ensure nosuid option set on /tmp partition (Automated)                                                                          | 95         |
| 1.1.2.1.4 Ensure noexec option set on /tmp partition (Automated)                                                                          | 97         |
| <b>1.1.2.2 Configure /dev/shm</b>                                                                                                         | <b>99</b>  |
| 1.1.2.2.1 Ensure /dev/shm is a separate partition (Automated)                                                                             | 100        |
| 1.1.2.2.2 Ensure nodev option set on /dev/shm partition (Automated)                                                                       | 102        |
| 1.1.2.2.3 Ensure nosuid option set on /dev/shm partition (Automated)                                                                      | 104        |
| 1.1.2.2.4 Ensure noexec option set on /dev/shm partition (Automated)                                                                      | 106        |
| <b>1.1.2.3 Configure /home</b>                                                                                                            | <b>108</b> |
| 1.1.2.3.1 Ensure separate partition exists for /home (Automated)                                                                          | 109        |
| 1.1.2.3.2 Ensure nodev option set on /home partition (Automated)                                                                          | 112        |
| 1.1.2.3.3 Ensure nosuid option set on /home partition (Automated)                                                                         | 114        |
| 1.1.2.3.4 Ensure a separate file system/partition has been created for non-privileged local interactive user home directories (Automated) | 116        |
| 1.1.2.3.5 Ensure file systems that contain user home directories are mounted with the nosuid option (Automated)                           | 118        |
| 1.1.2.3.6 Ensure file systems that contain user home directories are mounted with the "noexec" option (Automated)                         | 120        |
| <b>1.1.2.4 Configure /var</b>                                                                                                             | <b>122</b> |
| 1.1.2.4.1 Ensure separate partition exists for /var (Automated)                                                                           | 123        |
| 1.1.2.4.2 Ensure nodev option set on /var partition (Automated)                                                                           | 126        |
| 1.1.2.4.3 Ensure nosuid option set on /var partition (Automated)                                                                          | 128        |
| <b>1.1.2.5 Configure /var/tmp</b>                                                                                                         | <b>130</b> |
| 1.1.2.5.1 Ensure separate partition exists for /var/tmp (Automated)                                                                       | 131        |
| 1.1.2.5.2 Ensure nodev option set on /var/tmp partition (Automated)                                                                       | 133        |
| 1.1.2.5.3 Ensure nosuid option set on /var/tmp partition (Automated)                                                                      | 135        |
| 1.1.2.5.4 Ensure noexec option set on /var/tmp partition (Automated)                                                                      | 137        |
| <b>1.1.2.6 Configure /var/log</b>                                                                                                         | <b>139</b> |
| 1.1.2.6.1 Ensure separate partition exists for /var/log (Automated)                                                                       | 140        |
| 1.1.2.6.2 Ensure nodev option set on /var/log partition (Automated)                                                                       | 142        |
| 1.1.2.6.3 Ensure nosuid option set on /var/log partition (Automated)                                                                      | 144        |
| 1.1.2.6.4 Ensure noexec option set on /var/log partition (Automated)                                                                      | 146        |
| <b>1.1.2.7 Configure /var/log/audit</b>                                                                                                   | <b>148</b> |
| 1.1.2.7.1 Ensure separate partition exists for /var/log/audit (Automated)                                                                 | 149        |
| 1.1.2.7.2 Ensure nodev option set on /var/log/audit partition (Automated)                                                                 | 152        |
| 1.1.2.7.3 Ensure nosuid option set on /var/log/audit partition (Automated)                                                                | 154        |
| 1.1.2.7.4 Ensure noexec option set on /var/log/audit partition (Automated)                                                                | 156        |
| <b>1.1.2.8 Configure /boot</b>                                                                                                            | <b>158</b> |
| 1.1.2.8.1 Ensure the "/boot" directory is mounted with the "nosuid" option (Automated)                                                    | 159        |
| <b>1.1.2.9 Configure /boot/efi</b>                                                                                                        | <b>161</b> |
| 1.1.2.9.1 Ensure the "/boot/efi" directory is mounted with the "nosuid" option (Automated)                                                | 162        |
| <b>1.1.2.10 Configure nfs filesystems</b>                                                                                                 | <b>164</b> |



|                                                                                                                                                           |            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 1.1.2.10.1 Ensure file systems that are being NFS-imported are mounted with the "nodev" option (Automated) .....                                          | 165        |
| 1.1.2.10.2 Ensure file systems being imported via NFS are mounted with the "nosuid" option (Automated) .....                                              | 167        |
| 1.1.2.10.3 Ensure file systems being imported via NFS are mounted with the "noexec" option (Automated) .....                                              | 169        |
| <b>1.1.2.11 Configure removable media partitions.....</b>                                                                                                 | <b>171</b> |
| 1.1.2.11.1 Ensure nodev option set on removable media partitions (Manual) .....                                                                           | 172        |
| 1.1.2.11.2 Ensure nosuid option set on removable media partitions (Manual) .....                                                                          | 174        |
| 1.1.2.11.3 Ensure noexec option set on removable media partitions (Manual) .....                                                                          | 176        |
| 1.1.2.12 Ensure all non-root local partitions are mounted with the "nodev" option (Automated) .....                                                       | 178        |
| <b>1.1.3 Configure disk encryption.....</b>                                                                                                               | <b>180</b> |
| 1.1.3.1 Ensure all information at rest is encrypted (Manual) .....                                                                                        | 181        |
| <b>1.2 Package Management .....</b>                                                                                                                       | <b>184</b> |
| <b>1.2.1 Configure Package Repositories.....</b>                                                                                                          | <b>185</b> |
| 1.2.1.1 Ensure GPG keys are configured (Manual).....                                                                                                      | 186        |
| 1.2.1.2 Ensure gpgcheck is globally activated (Automated).....                                                                                            | 189        |
| 1.2.1.3 Ensure repo_gpgcheck is globally activated (Manual) .....                                                                                         | 192        |
| 1.2.1.4 Ensure package manager repositories are configured (Manual) .....                                                                                 | 194        |
| 1.2.1.5 Ensure DNF is configured to perform a signature check on local packages (Automated) .....                                                         | 196        |
| 1.2.1.6 Ensure cryptographic verification of vendor software packages (Manual) .....                                                                      | 198        |
| <b>1.2.2 Configure Package Updates .....</b>                                                                                                              | <b>200</b> |
| 1.2.2.1 Ensure updates, patches, and additional security software are installed (Manual) ...                                                              | 201        |
| 1.2.2.2 Ensure vendor packaged system security patches and updates are installed (Manual) .....                                                           | 203        |
| 1.2.2.3 Ensure Operating System is a vendor-supported release (Manual) .....                                                                              | 206        |
| 1.2.2.4 Ensure the operating system removes all software components after updated versions have been installed (Automated) .....                          | 207        |
| <b>1.3 Mandatory Access Control .....</b>                                                                                                                 | <b>209</b> |
| <b>1.3.1 Configure SELinux.....</b>                                                                                                                       | <b>210</b> |
| 1.3.1.1 Ensure SELinux is installed (Automated) .....                                                                                                     | 212        |
| 1.3.1.2 Ensure SELinux is not disabled in bootloader configuration (Automated) .....                                                                      | 214        |
| 1.3.1.3 Ensure SELinux policy is configured (Automated) .....                                                                                             | 217        |
| 1.3.1.4 Ensure the SELinux mode is not disabled (Automated) .....                                                                                         | 219        |
| 1.3.1.5 Ensure the SELinux mode is enforcing (Automated) .....                                                                                            | 222        |
| 1.3.1.6 Ensure no unconfined services exist (Manual).....                                                                                                 | 225        |
| 1.3.1.7 Ensure the MCS Translation Service (mcstrans) is not installed (Automated) .....                                                                  | 228        |
| 1.3.1.8 Ensure the operating system has the polycoreutils package installed (Automated).....                                                              | 230        |
| 1.3.1.9 Ensure SETroubleshoot is not installed (Automated).....                                                                                           | 232        |
| 1.3.1.10 Ensure SELinux prevents nonprivileged users from executing privileged functions (Manual).....                                                    | 234        |
| 1.3.1.11 Ensure SELinux targeted policy is configured (Manual).....                                                                                       | 237        |
| <b>1.4 Configure Bootloader .....</b>                                                                                                                     | <b>240</b> |
| 1.4.1 Ensure bootloader password is set (Automated).....                                                                                                  | 242        |
| 1.4.2 Ensure access to bootloader config is configured (Automated) .....                                                                                  | 245        |
| 1.4.3 Ensure the operating system requires authentication for rescue mode (Automated) ...                                                                 | 249        |
| 1.4.4 Ensure the operating system requires authentication upon booting into emergency mode (Automated) .....                                              | 251        |
| 1.4.5 Ensure a unique name is set as the superusers account (BIOS) (Automated).....                                                                       | 253        |
| 1.4.6 Ensure a unique name is set as the superusers account (UEFI) (Automated) .....                                                                      | 255        |
| 1.4.7 Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed seven times within two seconds (Automated) ..... | 257        |
| 1.4.8 Ensure GRUB 2 is configured to enable page poisoning to mitigate use-after-free vulnerabilities (Automated) .....                                   | 259        |

|                                                                                                                                             |            |
|---------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 1.4.9 Ensure GRUB 2 is configured to enable poisoning of SLUB/SLAB objects to mitigate use-after-free vulnerabilities (Automated).....      | 261        |
| 1.4.10 Ensure GRUB 2 is configured to disable vsyscalls (Automated).....                                                                    | 264        |
| <b>1.5 Configure Additional Process Hardening .....</b>                                                                                     | <b>266</b> |
| 1.5.1 Ensure address space layout randomization is enabled (Automated) .....                                                                | 267        |
| 1.5.2 Ensure ptrace_scope is restricted (Automated) .....                                                                                   | 271        |
| 1.5.3 Ensure core dump backtraces are disabled (Automated) .....                                                                            | 276        |
| 1.5.4 Ensure core dump storage is disabled (Automated) .....                                                                                | 280        |
| 1.5.5 Ensure the storing of core dumps is disabled (Automated).....                                                                         | 284        |
| 1.5.6 Ensure the operating system is not configured to acquire save or process core dumps (Automated) .....                                 | 286        |
| 1.5.7 Ensure kernel core dumps are disabled unless needed (Automated).....                                                                  | 288        |
| 1.5.8 Ensure the operating system enables hardening for the BPF JIT (Automated) .....                                                       | 290        |
| 1.5.9 Ensure kernel page-table isolation is enabled (Automated).....                                                                        | 294        |
| 1.5.10 Ensure the NX (no-execution) bit flag is set on the system (Automated).....                                                          | 297        |
| 1.5.11 Ensure the operating system disables the use of user namespaces (Automated) ....                                                     | 299        |
| 1.5.12 Ensure kernel image loading is disabled (Automated) .....                                                                            | 304        |
| 1.5.13 Ensure the operating system is configured to enable DAC on symlinks (Automated)                                                      | 308        |
| 1.5.14 Ensure the operating system is configured to boot to the command line (Manual) ....                                                  | 313        |
| 1.5.15 Ensure the operating system is configured to enable DAC on hardlinks (Automated)                                                     | 315        |
| 1.5.16 Ensure the operating system restricts exposed kernel pointer addresses access (Automated) .....                                      | 320        |
| 1.5.17 Ensure the operating system is configured to restrict access to the kernel message buffer (Automated) .....                          | 322        |
| 1.5.18 Ensure the operating system disables core dumps for all users (Automated) .....                                                      | 326        |
| 1.5.19 Ensure the operating system is configured to prevent kernel profiling by unprivileged users (Automated) .....                        | 328        |
| 1.5.20 Ensure the operating system restricts usage of ptrace to descendant processes (Automated) .....                                      | 332        |
| 1.5.21 Ensure the operating system prevents privilege escalation through the kernel by disabling access to the bpf syscall (Automated)..... | 337        |
| 1.5.22 Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed (Automated) .....                 | 342        |
| 1.5.23 Ensure the operating system implements the Endpoint Security for Linux Threat Prevention tool (Automated) .....                      | 344        |
| <b>1.6 Configure system wide crypto policy .....</b>                                                                                        | <b>346</b> |
| 1.6.1 Ensure system wide crypto policy is not set to legacy (Automated).....                                                                | 347        |
| 1.6.2 Ensure system wide crypto policy is not set in sshd configuration (Automated) .....                                                   | 350        |
| 1.6.3 Ensure system wide crypto policy disables sha1 hash and signature support (Automated) .....                                           | 352        |
| 1.6.4 Ensure system wide crypto policy disables macs less than 128 bits (Automated) .....                                                   | 355        |
| 1.6.5 Ensure system wide crypto policy disables cbc for ssh (Automated) .....                                                               | 358        |
| 1.6.6 Ensure system wide crypto policy disables chacha20-poly1305 for ssh (Manual) .....                                                    | 362        |
| 1.6.7 Ensure system wide crypto policy disables EtM for ssh (Manual).....                                                                   | 366        |
| 1.6.8 Ensure system-wide crypto policy is FIPS (Automated).....                                                                             | 369        |
| 1.6.9 Ensure PKI-based authentication has valid certificates (Manual) .....                                                                 | 373        |
| 1.6.10 Ensure system-wide crypto policies are in effect (Automated).....                                                                    | 376        |
| 1.6.11 Ensure the operating system implements certificate status checking for multifactor authentication (Automated).....                   | 378        |
| 1.6.12 Ensure the OpenSSL library is configured to use only ciphers employing FIPS 140-2-approved algorithms (Automated) .....              | 380        |
| 1.6.13 Ensure the OpenSSL library is configured to use only DoD-approved TLS encryption (Automated) .....                                   | 383        |
| 1.6.14 Ensure the GnuTLS library is configured to only allow DoD-approved SSL/TLS Versions (Automated) .....                                | 386        |
| <b>1.7 Configure Command Line Warning Banners .....</b>                                                                                     | <b>388</b> |

|                                                                                                                                                                                       |            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 1.7.1 Ensure message of the day is configured properly (Automated)                                                                                                                    | 389        |
| 1.7.2 Ensure local login warning banner is configured properly (Automated)                                                                                                            | 391        |
| 1.7.3 Ensure remote login warning banner is configured properly (Automated)                                                                                                           | 393        |
| 1.7.4 Ensure access to /etc/motd is configured (Automated)                                                                                                                            | 395        |
| 1.7.5 Ensure access to /etc/issue is configured (Automated)                                                                                                                           | 397        |
| 1.7.6 Ensure access to /etc/issue.net is configured (Automated)                                                                                                                       | 399        |
| 1.7.7 Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a command line user logon (Manual) | 401        |
| <b>1.8 Configure GNOME Display Manager</b>                                                                                                                                            | <b>406</b> |
| 1.8.1 Ensure GNOME Display Manager is removed (Automated)                                                                                                                             | 407        |
| 1.8.2 Ensure GDM login banner is configured (Automated)                                                                                                                               | 409        |
| 1.8.3 Ensure GDM disable-user-list option is enabled (Automated)                                                                                                                      | 413        |
| 1.8.4 Ensure GDM screen locks when the user is idle (Automated)                                                                                                                       | 417        |
| 1.8.5 Ensure GDM screen locks cannot be overridden (Automated)                                                                                                                        | 422        |
| 1.8.6 Ensure GDM automatic mounting of removable media is disabled (Automated)                                                                                                        | 427        |
| 1.8.7 Ensure GDM disabling automatic mounting of removable media is not overridden (Automated)                                                                                        | 433        |
| 1.8.8 Ensure the operating system does not allow an unattended or automatic logon to the system via a graphical user interface (Automated)                                            | 438        |
| 1.8.9 Ensure GDM autorun-never is enabled (Automated)                                                                                                                                 | 440        |
| 1.8.10 Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed when using a graphical user interface (Automated)                           | 445        |
| 1.8.11 Ensure GDM autorun-never is not overridden (Automated)                                                                                                                         | 447        |
| 1.8.12 Ensure the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated (Automated)                                             | 452        |
| 1.8.13 Ensure XDMCP is not enabled (Automated)                                                                                                                                        | 454        |
| 1.8.14 Ensure the operating system disables the user logon list for graphical user interfaces (Automated)                                                                             | 456        |
| 1.8.15 Ensure GDM login banner displays the Mandatory DoD Notice and Consent Banner (Manual)                                                                                          | 459        |
| 1.8.16 Ensure the operating system prevents users from overriding the session idle-delay setting for the graphical user interface (Automated)                                         | 464        |
| 1.8.17 Ensure the operating system prevents users from overriding the screensaver lock-enabled setting for the graphical user interface (Automated)                                   | 467        |
| 1.8.18 Ensure the operating system initiates a session lock for all connection types using smartcard when the smartcard is removed (Manual)                                           | 470        |
| 1.8.19 Ensure the operating system enables a user's session lock until that user re-establishes access (Automated)                                                                    | 472        |
| 1.9 Ensure the "tmux" package installed (Automated)                                                                                                                                   | 474        |
| 1.10 Ensure the system has the packages required to enable the hardware random number generator entropy gatherer service (Automated)                                                  | 476        |
| 1.11 Ensure the mailx package is installed (Automated)                                                                                                                                | 478        |
| 1.12 Ensure the operating system accepts PIV credentials (Automated)                                                                                                                  | 480        |
| 1.13 Ensure the operating system has the packages required for multifactor authentication (Automated)                                                                                 | 482        |
| <b>2 Services</b>                                                                                                                                                                     | <b>484</b> |
| <b>2.1 Configure Server Services</b>                                                                                                                                                  | <b>485</b> |
| 2.1.1 Ensure autofs services are not in use (Automated)                                                                                                                               | 486        |
| 2.1.2 Ensure avahi daemon services are not in use (Automated)                                                                                                                         | 489        |
| 2.1.3 Ensure dhcp server services are not in use (Automated)                                                                                                                          | 492        |
| 2.1.4 Ensure dns server services are not in use (Automated)                                                                                                                           | 495        |
| 2.1.5 Ensure dnsmasq services are not in use (Automated)                                                                                                                              | 498        |
| 2.1.6 Ensure ftp server services are not in use (Automated)                                                                                                                           | 501        |
| 2.1.7 Ensure message access server services are not in use (Automated)                                                                                                                | 504        |

|                                                                                                                                                           |            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 2.1.8 Ensure network file system services are not in use (Automated).....                                                                                 | 507        |
| 2.1.9 Ensure nis server services are not in use (Automated).....                                                                                          | 510        |
| 2.1.10 Ensure print server services are not in use (Automated) .....                                                                                      | 513        |
| 2.1.11 Ensure rpcbind services are not in use (Automated).....                                                                                            | 516        |
| 2.1.12 Ensure rsync services are not in use (Automated).....                                                                                              | 519        |
| 2.1.13 Ensure samba file server services are not in use (Automated).....                                                                                  | 522        |
| 2.1.14 Ensure snmp services are not in use (Automated).....                                                                                               | 525        |
| 2.1.15 Ensure telnet server services are not in use (Automated) .....                                                                                     | 528        |
| 2.1.16 Ensure tftp server services are not in use (Automated) .....                                                                                       | 531        |
| 2.1.17 Ensure web proxy server services are not in use (Automated).....                                                                                   | 534        |
| 2.1.18 Ensure web server services are not in use (Automated).....                                                                                         | 537        |
| 2.1.19 Ensure xinetd services are not in use (Automated).....                                                                                             | 540        |
| 2.1.20 Ensure X window server services are not in use (Automated).....                                                                                    | 543        |
| 2.1.21 Ensure only approved services are listening on a network interface (Manual) .....                                                                  | 545        |
| 2.1.22 Ensure automated bug reporting tools are not installed (Automated) .....                                                                           | 548        |
| 2.1.23 Ensure mail transfer agents are configured for local-only mode (Automated) .....                                                                   | 550        |
| 2.1.24 Ensure the sendmail package is not installed (Automated) .....                                                                                     | 553        |
| 2.1.25 Ensure the rsh-server package is not installed (Automated).....                                                                                    | 555        |
| 2.1.26 Ensure system daemons are prevented from using Kerberos for authentication<br>(Automated) .....                                                    | 557        |
| 2.1.27 Ensure the operating system is configured to mask the debug-shell systemd service<br>(Automated) .....                                             | 559        |
| 2.1.28 Ensure the gssproxy package has not been installed on the system (Automated).....                                                                  | 561        |
| 2.1.29 Ensure the iprutils package has not been installed on the system (Automated).....                                                                  | 563        |
| 2.1.30 Ensure the krb5-server package has not been installed on the system (Automated).....                                                               | 565        |
| 2.1.31 Ensure a TFTP server has not been installed on the system (Automated).....                                                                         | 567        |
| 2.1.32 Ensure the tuned package has not been installed on the system (Automated) .....                                                                    | 569        |
| 2.1.33 Ensure the operating system has enabled the hardware random number generator<br>entropy gatherer service (Automated) .....                         | 571        |
| 2.1.34 Ensure the operating system is configured to prevent unrestricted mail relaying<br>(Automated) .....                                               | 573        |
| 2.1.35 Ensure the TFTP daemon is configured to operate in secure mode (Automated).....                                                                    | 575        |
| <b>2.2 Configure Client Services .....</b>                                                                                                                | <b>577</b> |
| 2.2.1 Ensure ftp client is not installed (Automated) .....                                                                                                | 578        |
| 2.2.2 Ensure ldap client is not installed (Automated) .....                                                                                               | 580        |
| 2.2.3 Ensure nis client is not installed (Automated).....                                                                                                 | 582        |
| 2.2.4 Ensure telnet client is not installed (Automated) .....                                                                                             | 584        |
| 2.2.5 Ensure tftp client is not installed (Automated) .....                                                                                               | 586        |
| 2.2.6 Ensure krb5-workstation is not installed (Automated) .....                                                                                          | 588        |
| <b>2.3 Configure Time Synchronization .....</b>                                                                                                           | <b>590</b> |
| 2.3.1 Ensure time synchronization is in use (Automated) .....                                                                                             | 591        |
| 2.3.2 Ensure chrony is configured (Automated) .....                                                                                                       | 593        |
| 2.3.3 Ensure chrony is not run as the root user (Automated).....                                                                                          | 597        |
| 2.3.4 Ensure the operating system is securely comparing internal information system clocks at<br>least every 24 hours with an NTP server (Automated)..... | 598        |
| 2.3.5 Ensure the operating system disables network management of the chrony daemon<br>(Automated) .....                                                   | 601        |
| 2.3.6 Ensure the operating system disables the chrony daemon from acting as a server<br>(Automated) .....                                                 | 603        |
| <b>2.4 Job Schedulers .....</b>                                                                                                                           | <b>605</b> |
| <b>2.4.1 Configure cron.....</b>                                                                                                                          | <b>606</b> |
| 2.4.1.1 Ensure cron daemon is enabled and active (Automated) .....                                                                                        | 607        |
| 2.4.1.2 Ensure permissions on /etc/crontab are configured (Automated) .....                                                                               | 609        |
| 2.4.1.3 Ensure permissions on /etc/cron.hourly are configured (Automated) .....                                                                           | 611        |
| 2.4.1.4 Ensure permissions on /etc/cron.daily are configured (Automated).....                                                                             | 613        |
| 2.4.1.5 Ensure permissions on /etc/cron.weekly are configured (Automated) .....                                                                           | 615        |

|                                                                                                                                    |            |
|------------------------------------------------------------------------------------------------------------------------------------|------------|
| 2.4.1.6 Ensure permissions on /etc/cron.monthly are configured (Automated).....                                                    | 617        |
| 2.4.1.7 Ensure permissions on /etc/cron.d are configured (Automated) .....                                                         | 619        |
| 2.4.1.8 Ensure crontab is restricted to authorized users (Automated) .....                                                         | 621        |
| <b>2.4.2 Configure at .....</b>                                                                                                    | <b>625</b> |
| 2.4.2.1 Ensure at is restricted to authorized users (Automated) .....                                                              | 626        |
| <b>2.5 Configure USBGuard.....</b>                                                                                                 | <b>630</b> |
| 2.5.1 Ensure USBGuard is installed on the operating system (Automated).....                                                        | 631        |
| 2.5.2 Ensure USBGuard has a policy configured (Manual).....                                                                        | 633        |
| 2.5.3 Ensure the operating system enables Linux audit logging of the USBGuard daemon<br>(Automated) .....                          | 635        |
| 2.5.4 Ensure the usbguard service is enabled and active (Automated) .....                                                          | 637        |
| <b>2.6 Configure fapolicyd .....</b>                                                                                               | <b>639</b> |
| 2.6.1 Ensure fapolicyd is installed (Automated) .....                                                                              | 640        |
| 2.6.2 Ensure fapolicyd employs a deny-all, permit-by-exception policy (Automated) .....                                            | 642        |
| 2.6.3 Ensure fapolicyd is enabled and running (Automated).....                                                                     | 645        |
| <b>3 Network .....</b>                                                                                                             | <b>647</b> |
| <b>3.1 Configure Network Devices .....</b>                                                                                         | <b>648</b> |
| 3.1.1 Ensure IPv6 status is identified (Manual) .....                                                                              | 649        |
| 3.1.2 Ensure wireless interfaces are disabled (Automated) .....                                                                    | 652        |
| 3.1.3 Ensure bluetooth services are not in use (Automated).....                                                                    | 656        |
| 3.1.4 Ensure network interfaces are not in promiscuous mode (Manual) .....                                                         | 659        |
| <b>3.2 Configure Network Kernel Modules .....</b>                                                                                  | <b>661</b> |
| 3.2.1 Ensure dccp kernel module is not available (Automated) .....                                                                 | 662        |
| 3.2.2 Ensure tipc kernel module is not available (Automated) .....                                                                 | 667        |
| 3.2.3 Ensure rds kernel module is not available (Automated) .....                                                                  | 672        |
| 3.2.4 Ensure sctp kernel module is not available (Automated) .....                                                                 | 677        |
| 3.2.5 Ensure atm kernel module is not available (Automated) .....                                                                  | 682        |
| 3.2.6 Ensure bluetooth kernel module is not available (Automated) .....                                                            | 687        |
| 3.2.7 Ensure can kernel module is not available (Automated) .....                                                                  | 693        |
| <b>3.3 Configure Network Kernel Parameters .....</b>                                                                               | <b>698</b> |
| 3.3.1 Ensure ip forwarding is disabled (Automated) .....                                                                           | 699        |
| 3.3.2 Ensure packet redirect sending is disabled (Automated) .....                                                                 | 704        |
| 3.3.3 Ensure bogus icmp responses are ignored (Automated) .....                                                                    | 709        |
| 3.3.4 Ensure broadcast icmp requests are ignored (Automated) .....                                                                 | 714        |
| 3.3.5 Ensure icmp redirects are not accepted (Automated) .....                                                                     | 719        |
| 3.3.6 Ensure secure icmp redirects are not accepted (Automated) .....                                                              | 725        |
| 3.3.7 Ensure reverse path filtering is enabled (Automated) .....                                                                   | 730        |
| 3.3.8 Ensure source routed packets are not accepted (Automated) .....                                                              | 735        |
| 3.3.9 Ensure suspicious packets are logged (Automated) .....                                                                       | 742        |
| 3.3.10 Ensure tcp syn cookies is enabled (Automated) .....                                                                         | 747        |
| 3.3.11 Ensure ipv6 router advertisements are not accepted (Automated) .....                                                        | 752        |
| 3.3.12 Ensure net.ipv4.conf.all.forwarding is disabled (Automated) .....                                                           | 757        |
| 3.4 Ensure at least two name servers are configured if using DNS resolution (Automated) ..                                         | 760        |
| <b>4 Host Based Firewall.....</b>                                                                                                  | <b>762</b> |
| <b>4.1 Configure a firewall utility.....</b>                                                                                       | <b>763</b> |
| <b>4.1.1 Configure firewall rules .....</b>                                                                                        | <b>764</b> |
| 4.1.1.1 Ensure nftables base chains exist (Automated) .....                                                                        | 768        |
| 4.1.1.2 Ensure host based firewall loopback traffic is configured (Automated).....                                                 | 771        |
| 4.1.1.3 Ensure firewalld drops unnecessary services and ports (Manual) .....                                                       | 775        |
| 4.1.1.4 Ensure nftables established connections are configured (Manual).....                                                       | 777        |
| 4.1.1.5 Ensure nftables default deny firewall policy (Automated).....                                                              | 779        |
| 4.1.2 Ensure the firewall is configured to remove unnecessary use of functions, ports,<br>protocols, and/or services (Manual)..... | 781        |
| 4.1.3 Ensure firewalld service is enabled and running (Automated) .....                                                            | 784        |
| 4.1.4 Ensure nftables is installed (Automated) .....                                                                               | 786        |

|                                                                                                                                                   |            |
|---------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 4.1.5 Ensure a single firewall configuration utility is in use (Automated).....                                                                   | 788        |
| 4.1.6 Ensure "nftables" is configured to allow rate limits on any connection to the system<br>(Automated) .....                                   | 792        |
| 4.1.7 Ensure "firewalld" is installed (Automated).....                                                                                            | 794        |
| 4.1.8 Ensure "firewalld" is configured to employ a deny-all, allow-by-exception policy for<br>allowing connections to other systems (Manual)..... | 796        |
| <b>5 Access Control .....</b>                                                                                                                     | <b>798</b> |
| <b>5.1 Configure SSH Server .....</b>                                                                                                             | <b>799</b> |
| 5.1.1 Ensure openssh-server is installed (Automated).....                                                                                         | 801        |
| 5.1.2 Ensure permissions on /etc/ssh/sshd_config are configured (Automated) .....                                                                 | 803        |
| 5.1.3 Ensure permissions on SSH private host key files are configured (Automated) .....                                                           | 806        |
| 5.1.4 Ensure permissions on SSH public host key files are configured (Automated) .....                                                            | 810        |
| 5.1.5 Ensure sshd access is configured (Automated) .....                                                                                          | 814        |
| 5.1.6 Ensure sshd Banner is configured (Automated).....                                                                                           | 818        |
| 5.1.7 Ensure sshd Ciphers are configured (Automated) .....                                                                                        | 821        |
| 5.1.8 Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured (Automated)<br>.....                                                 | 825        |
| 5.1.9 Ensure sshd DisableForwarding is enabled (Automated) .....                                                                                  | 828        |
| 5.1.10 Ensure sshd GSSAPIAuthentication is disabled (Automated) .....                                                                             | 831        |
| 5.1.11 Ensure sshd HostbasedAuthentication is disabled (Automated).....                                                                           | 834        |
| 5.1.12 Ensure sshd IgnoreRhosts is enabled (Automated).....                                                                                       | 836        |
| 5.1.13 Ensure sshd KexAlgorithms is configured (Automated) .....                                                                                  | 838        |
| 5.1.14 Ensure sshd LoginGraceTime is configured (Automated).....                                                                                  | 842        |
| 5.1.15 Ensure sshd LogLevel is configured (Automated).....                                                                                        | 844        |
| 5.1.16 Ensure sshd MACs are configured (Automated).....                                                                                           | 846        |
| 5.1.17 Ensure sshd MaxAuthTries is configured (Automated) .....                                                                                   | 850        |
| 5.1.18 Ensure sshd MaxSessions is configured (Automated).....                                                                                     | 852        |
| 5.1.19 Ensure sshd MaxStartups is configured (Automated) .....                                                                                    | 854        |
| 5.1.20 Ensure sshd PermitEmptyPasswords is disabled (Automated) .....                                                                             | 856        |
| 5.1.21 Ensure sshd PermitRootLogin is disabled (Automated).....                                                                                   | 859        |
| 5.1.22 Ensure sshd PermitUserEnvironment is disabled (Automated) .....                                                                            | 862        |
| 5.1.23 Ensure sshd UsePAM is enabled (Automated) .....                                                                                            | 864        |
| 5.1.24 Ensure sshd private key files have a passcode (Manual) .....                                                                               | 866        |
| 5.1.25 Ensure sshd X11Forwarding is disabled (Automated) .....                                                                                    | 868        |
| 5.1.26 Ensure sshd ClientAliveInterval is configured (Automated) .....                                                                            | 870        |
| 5.1.27 Ensure sshd ClientAliveCountMax is configured (Automated).....                                                                             | 873        |
| 5.1.28 Ensure the SSH server is configured to use only MACs employing FIPS 140-2-<br>approved algorithms (Automated) .....                        | 876        |
| 5.1.29 Ensure the SSH server is configured to use only ciphers employing FIPS 140-2-<br>approved algorithms (Automated) .....                     | 879        |
| 5.1.30 Ensure sshd is configured to use only FIPS-validated key exchange algorithms<br>(Automated) .....                                          | 881        |
| 5.1.31 Ensure the SSH server uses strong entropy (Automated) .....                                                                                | 883        |
| 5.1.32 Ensure sshd StrictModes is enabled (Automated) .....                                                                                       | 885        |
| 5.1.33 Ensure sshd Banner is configured to display the Standard Mandatory DoD Notice and<br>Consent Banner (Manual).....                          | 887        |
| 5.1.34 Ensure sshd IgnoreUserKnownHosts is enabled (Automated) .....                                                                              | 892        |
| 5.1.35 Ensure sshd X11UseLocalhost is enabled (Automated) .....                                                                                   | 894        |
| 5.1.36 Ensure sshd KerberosAuthentication is disabled (Automated) .....                                                                           | 896        |
| 5.1.37 Ensure sshd RekeyLimit is configured (Automated).....                                                                                      | 898        |
| 5.1.38 Ensure sshd PrintLastLog is enabled (Automated) .....                                                                                      | 901        |
| 5.1.39 Ensure SSH is loaded and active (Automated) .....                                                                                          | 903        |
| <b>5.2 Configure privilege escalation .....</b>                                                                                                   | <b>905</b> |
| 5.2.1 Ensure sudo is installed (Automated).....                                                                                                   | 906        |
| 5.2.2 Ensure the sudoers file has the default include directory (Automated) .....                                                                 | 908        |

|                                                                                                                                                          |             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| 5.2.3 Ensure sudo commands use pty (Automated) .....                                                                                                     | 910         |
| 5.2.4 Ensure sudo log file exists (Automated) .....                                                                                                      | 913         |
| 5.2.5 Ensure users must provide password for escalation (Automated) .....                                                                                | 916         |
| 5.2.6 Ensure the sudoers file restricts sudo access to authorized personnel (Automated) ...                                                              | 918         |
| 5.2.7 Ensure re-authentication for privilege escalation is not disabled globally (Automated)                                                             | 920         |
| 5.2.8 Ensure the sudoers security policy is configured to use the invoking user's password for<br>privilege escalation (Automated) .....                 | 922         |
| 5.2.9 Ensure sudo timestamp_timeout is configured (Automated).....                                                                                       | 924         |
| 5.2.10 Ensure access to the su command is restricted (Automated) .....                                                                                   | 926         |
| 5.2.11 Ensure pam_succeed_if does not exist in /etc/pam.d/sudo (Automated) .....                                                                         | 928         |
| <b>5.3 Pluggable Authentication Modules .....</b>                                                                                                        | <b>930</b>  |
| <b>5.3.1 Configure PAM software packages .....</b>                                                                                                       | <b>931</b>  |
| 5.3.1.1 Ensure latest version of pam is installed (Automated) .....                                                                                      | 932         |
| 5.3.1.2 Ensure latest version of authselect is installed (Automated) .....                                                                               | 933         |
| <b>5.3.2 Configure authselect .....</b>                                                                                                                  | <b>935</b>  |
| 5.3.2.1 Ensure active authselect profile includes pam modules (Automated).....                                                                           | 937         |
| 5.3.2.2 Ensure pam_faillock module is enabled (Automated) .....                                                                                          | 942         |
| 5.3.2.3 Ensure pam_pwquality module is enabled (Automated) .....                                                                                         | 945         |
| 5.3.2.4 Ensure pam_pwhistory module is enabled (Automated) .....                                                                                         | 948         |
| 5.3.2.5 Ensure pam_unix module is enabled (Automated).....                                                                                               | 951         |
| <b>5.3.3 Configure PAM Arguments .....</b>                                                                                                               | <b>954</b>  |
| <b>5.3.3.1 Configure pam_faillock module .....</b>                                                                                                       | <b>955</b>  |
| 5.3.3.1.1 Ensure password failed attempts lockout is configured (Automated).....                                                                         | 957         |
| 5.3.3.1.2 Ensure password unlock time is configured (Automated) .....                                                                                    | 960         |
| 5.3.3.1.3 Ensure password failed attempts lockout includes root account (Automated) .....                                                                | 963         |
| 5.3.3.1.4 Ensure deny is configured on the pam_faillock module (Automated) .....                                                                         | 967         |
| 5.3.3.1.5 Ensure deny is configured in /etc/security/faillock.conf (Automated) .....                                                                     | 970         |
| 5.3.3.1.6 Ensure fail_interval is configured on the pam_faillock module (Automated).....                                                                 | 972         |
| 5.3.3.1.7 Ensure fail_interval is configured in /etc/security/faillock.conf (Automated).....                                                             | 975         |
| 5.3.3.1.8 Ensure unlock_time is configured on the pam_faillock module (Automated).....                                                                   | 977         |
| 5.3.3.1.9 Ensure unlock_time is configured in /etc/security/faillock.conf (Automated).....                                                               | 980         |
| 5.3.3.1.10 Ensure dir is configured on the pam_faillock module (Automated) .....                                                                         | 982         |
| 5.3.3.1.11 Ensure dir is configured in /etc/security/faillock.conf (Automated) .....                                                                     | 985         |
| 5.3.3.1.12 Ensure silent is set on the pam_faillock module (Automated).....                                                                              | 987         |
| 5.3.3.1.13 Ensure silent is set in /etc/security/faillock.conf (Automated).....                                                                          | 990         |
| 5.3.3.1.14 Ensure audit is set on the pam_faillock module (Automated) .....                                                                              | 992         |
| 5.3.3.1.15 Ensure audit is set in /etc/security/faillock.conf (Automated) .....                                                                          | 995         |
| 5.3.3.1.16 Ensure even_deny_root is set on the pam_faillock module (Automated) .....                                                                     | 997         |
| 5.3.3.1.17 Ensure even_deny_root is set in /etc/security/faillock.conf (Automated) .....                                                                 | 1000        |
| 5.3.3.1.18 Ensure the use of a non-default faillock tally directory while SELinux enforces a<br>targeted policy (Manual) .....                           | 1002        |
| 5.3.3.1.19 Ensure the use of a non-default faillock tally directory on the pam_faillock module<br>while SELinux enforces a targeted policy (Manual)..... | 1005        |
| <b>5.3.3.2 Configure pam_pwquality module.....</b>                                                                                                       | <b>1008</b> |
| 5.3.3.2.1 Ensure password number of changed characters is configured (Automated) .....                                                                   | 1009        |
| 5.3.3.2.2 Ensure password length is configured (Automated).....                                                                                          | 1013        |
| 5.3.3.2.3 Ensure password complexity is configured (Manual) .....                                                                                        | 1017        |
| 5.3.3.2.4 Ensure password same consecutive characters is configured (Automated).....                                                                     | 1021        |
| 5.3.3.2.5 Ensure password maximum sequential characters is configured (Automated) ....                                                                   | 1025        |
| 5.3.3.2.6 Ensure password dictionary check is enabled (Automated).....                                                                                   | 1029        |
| 5.3.3.2.7 Ensure password quality is enforced for the root user (Automated) .....                                                                        | 1033        |
| 5.3.3.2.8 Ensure the operating system enforces a minimum 15-character password length<br>(Automated) .....                                               | 1036        |
| 5.3.3.2.9 Ensure ucredit is configured in /etc/security/pwquality.conf (Automated) .....                                                                 | 1038        |
| 5.3.3.2.10 Ensure lcredit is configured in /etc/security/pwquality.conf (Automated) .....                                                                | 1040        |
| 5.3.3.2.11 Ensure dcredit is configured in /etc/security/pwquality.conf (Automated) .....                                                                | 1042        |

|                                                                                                                                           |             |
|-------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| 5.3.3.2.12 Ensure ocredit is configured in /etc/security/pwquality.conf (Automated) .....                                                 | 1044        |
| 5.3.3.2.13 Ensure maxclassrepeat is configured in /etc/security/pwquality.conf (Automated) .....                                          | 1046        |
| 5.3.3.2.14 Ensure minclass is configured in /etc/security/pwquality.conf (Automated) .....                                                | 1048        |
| 5.3.3.2.15 Ensure difok is configured in /etc/security/pwquality.conf (Automated) .....                                                   | 1050        |
| 5.3.3.2.16 Ensure dictcheck is configured (Automated) .....                                                                               | 1052        |
| 5.3.3.2.17 Ensure retry is configured on the pam_pwquality module in /etc/pam.d/system-auth (Automated) .....                             | 1054        |
| 5.3.3.2.18 Ensure retry is configured on the pam_pwquality module in /etc/pam.d/password-auth (Automated) .....                           | 1056        |
| 5.3.3.2.19 Ensure retry is configured in /etc/security/pwquality.conf (Automated) .....                                                   | 1058        |
| <b>5.3.3.3 Configure pam_pwhistory module .....</b>                                                                                       | <b>1060</b> |
| 5.3.3.3.1 Ensure password history remember is configured (Automated) .....                                                                | 1062        |
| 5.3.3.3.2 Ensure password history is enforced for the root user (Automated) .....                                                         | 1065        |
| 5.3.3.3.3 Ensure pam_pwhistory includes use_authok (Automated) .....                                                                      | 1067        |
| 5.3.3.3.4 Ensure remember is configured on the pam_pwhistory module in /etc/pam.d/password-auth (Automated) .....                         | 1070        |
| 5.3.3.3.5 Ensure remember is configured on the pam_pwhistory module in /etc/pam.d/system-auth (Automated) .....                           | 1072        |
| <b>5.3.3.4 Configure pam_unix module .....</b>                                                                                            | <b>1074</b> |
| 5.3.3.4.1 Ensure pam_unix does not include nullok (Automated) .....                                                                       | 1075        |
| 5.3.3.4.2 Ensure pam_unix does not include remember (Automated) .....                                                                     | 1078        |
| 5.3.3.4.3 Ensure pam_unix includes a strong password hashing algorithm (Automated) ...                                                    | 1081        |
| 5.3.3.4.4 Ensure pam_unix includes use_authok (Automated) .....                                                                           | 1085        |
| 5.3.3.4.5 Ensure pam_unix includes a FIPS 140-2 approved hashing algorithm (Automated) .....                                              | 1088        |
| <b>5.3.3.5 Configure pam_lastlog module .....</b>                                                                                         | <b>1092</b> |
| 5.3.3.5.1 Ensure the date and time of the last successful account login upon login is displayed (Automated) .....                         | 1093        |
| <b>5.3.3.6 Configure pam_sss module .....</b>                                                                                             | <b>1095</b> |
| 5.3.3.6.1 Ensure the operating system uses multifactor authentication for local access to accounts (Automated) .....                      | 1096        |
| 5.3.3.6.2 Ensure SSSD prohibits the use of cached authentications after one day (Automated) .....                                         | 1099        |
| 5.3.3.6.3 Ensure the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file (Manual) ..... | 1101        |
| <b>5.4 User Accounts and Environment .....</b>                                                                                            | <b>1103</b> |
| <b>5.4.1 Configure shadow password suite parameters .....</b>                                                                             | <b>1104</b> |
| 5.4.1.1 Ensure password expiration is configured (Automated) .....                                                                        | 1105        |
| 5.4.1.2 Ensure minimum password days is configured (Automated) .....                                                                      | 1109        |
| 5.4.1.3 Ensure password expiration warning days is configured (Automated) .....                                                           | 1112        |
| 5.4.1.4 Ensure strong password hashing algorithm is configured (Automated) .....                                                          | 1114        |
| 5.4.1.5 Ensure inactive password lock is configured (Automated) .....                                                                     | 1117        |
| 5.4.1.6 Ensure all users last password change date is in the past (Automated) .....                                                       | 1120        |
| 5.4.1.7 Ensure passwords use FIPS 140-2 approved cryptographic hashing algorithm (Automated) .....                                        | 1122        |
| 5.4.1.8 Ensure minimum number of hashing rounds is configured (Automated) .....                                                           | 1125        |
| 5.4.1.9 Ensure existing passwords use FIPS 140-2 approved cryptographic hashing algorithm (Automated) .....                               | 1128        |
| 5.4.1.10 Ensure temporary accounts have been provisioned with an expiration date of 72 hours (Manual) .....                               | 1132        |
| 5.4.1.11 Ensure fail_delay is configured (Automated) .....                                                                                | 1134        |
| 5.4.1.12 Ensure pass_min_len is configured (Automated) .....                                                                              | 1136        |
| 5.4.1.13 Ensure the maximum time period for existing passwords is restricted to 60 days (Automated) .....                                 | 1138        |
| <b>5.4.2 Configure root and system accounts and environment .....</b>                                                                     | <b>1140</b> |



|                                                                                                                                                                                    |             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| 5.4.2.1 Ensure root is the only UID 0 account (Automated) .....                                                                                                                    | 1141        |
| 5.4.2.2 Ensure root is the only GID 0 account (Automated) .....                                                                                                                    | 1143        |
| 5.4.2.3 Ensure group root is the only GID 0 group (Automated) .....                                                                                                                | 1145        |
| 5.4.2.4 Ensure root account access is controlled (Automated) .....                                                                                                                 | 1147        |
| 5.4.2.5 Ensure root path integrity (Automated) .....                                                                                                                               | 1149        |
| 5.4.2.6 Ensure root user umask is configured (Automated) .....                                                                                                                     | 1152        |
| 5.4.2.7 Ensure system accounts do not have a valid login shell (Automated) .....                                                                                                   | 1155        |
| 5.4.2.8 Ensure accounts without a valid login shell are locked (Automated) .....                                                                                                   | 1158        |
| 5.4.2.9 Ensure all accounts on the system are assigned to an active system, application, or user account (Manual) .....                                                            | 1160        |
| <b>5.4.3 Configure user default environment .....</b>                                                                                                                              | <b>1162</b> |
| 5.4.3.1 Ensure nologin is not listed in /etc/shells (Automated) .....                                                                                                              | 1163        |
| 5.4.3.2 Ensure default user shell timeout is configured (Automated) .....                                                                                                          | 1164        |
| 5.4.3.3 Ensure default user umask is configured (Automated) .....                                                                                                                  | 1168        |
| 5.4.3.4 Ensure emergency accounts have been provisioned with an expiration date of 72 hours (Manual) .....                                                                         | 1175        |
| 5.4.3.5 Ensure the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity (Automated) .....                                        | 1177        |
| 5.4.3.6 Ensure the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files (Automated) ..... | 1179        |
| 5.4.3.7 Ensure the operating system enforces a 60-day maximum password lifetime for new user accounts (Automated) .....                                                            | 1181        |
| 5.4.3.8 Ensure the umask default for installed shells is "077" (Automated) .....                                                                                                   | 1183        |
| 5.4.3.9 Ensure the default umask for all local interactive users is "077" (Manual) .....                                                                                           | 1185        |
| 5.4.3.10 Ensure the operating system initiates a session lock after 15 minutes of inactivity (Automated) .....                                                                     | 1187        |
| 5.4.3.11 Ensure the operating system prevents users from disabling the tmux terminal multiplexer (Automated) .....                                                                 | 1189        |
| 5.4.3.12 Ensure the operating system's shell initialization file is configured to start each shell with the tmux terminal multiplexer (Automated) .....                            | 1191        |
| 5.4.3.13 Ensure the operating system enables the user to initiate a session lock (Automated) .....                                                                                 | 1194        |
| 5.4.3.14 Ensure the number of concurrent sessions is configured (Automated) .....                                                                                                  | 1196        |
| 5.4.3.15 Ensure all local interactive users are assigned a home directory upon creation (Automated) .....                                                                          | 1198        |
| 5.4.3.16 Ensure StopIdleSessionSec is configured (Automated) .....                                                                                                                 | 1200        |
| <b>6 Logging and Auditing .....</b>                                                                                                                                                | <b>1202</b> |
| <b>6.1 Configure Integrity Checking .....</b>                                                                                                                                      | <b>1203</b> |
| 6.1.1 Ensure AIDE is installed (Automated) .....                                                                                                                                   | 1204        |
| 6.1.2 Ensure filesystem integrity is regularly checked (Automated) .....                                                                                                           | 1206        |
| 6.1.3 Ensure cryptographic mechanisms are used to protect the integrity of audit tools (Automated) .....                                                                           | 1209        |
| 6.1.4 Ensure AIDE is configured to use cryptographic mechanisms to protect the integrity of audit tools (Automated) .....                                                          | 1214        |
| 6.1.5 Ensure the file integrity tool is configured to verify ACLs (Manual) .....                                                                                                   | 1217        |
| 6.1.6 Ensure the file integrity tool is configured to verify extended attributes (Manual) .....                                                                                    | 1219        |
| <b>6.2 System Logging .....</b>                                                                                                                                                    | <b>1221</b> |
| <b>6.2.1 Configure journald .....</b>                                                                                                                                              | <b>1222</b> |
| <b>6.2.1.1 Configure systemd-journald service .....</b>                                                                                                                            | <b>1223</b> |
| 6.2.1.1.1 Ensure journald service is enabled and active (Automated) .....                                                                                                          | 1224        |
| 6.2.1.1.2 Ensure journald log file access is configured (Manual) .....                                                                                                             | 1226        |
| 6.2.1.1.3 Ensure journald log file rotation is configured (Manual) .....                                                                                                           | 1229        |
| 6.2.1.1.4 Ensure journald ForwardToSyslog is disabled (Automated) .....                                                                                                            | 1231        |
| 6.2.1.1.5 Ensure journald Storage is configured (Automated) .....                                                                                                                  | 1235        |
| 6.2.1.1.6 Ensure journald Compress is configured (Automated) .....                                                                                                                 | 1239        |

|                                                                                                                                                               |             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| <b>6.2.1.2 Configure systemd-journal-remote</b> .....                                                                                                         | <b>1243</b> |
| 6.2.1.2.1 Ensure systemd-journal-remote is installed (Automated).....                                                                                         | 1244        |
| 6.2.1.2.2 Ensure systemd-journal-remote authentication is configured (Manual) .....                                                                           | 1246        |
| 6.2.1.2.3 Ensure systemd-journal-upload is enabled and active (Automated) .....                                                                               | 1248        |
| 6.2.1.2.4 Ensure systemd-journal-remote service is not in use (Automated).....                                                                                | 1250        |
| <b>6.2.2 Configure rsyslog</b> .....                                                                                                                          | <b>1252</b> |
| 6.2.2.1 Ensure rsyslog is installed (Automated) .....                                                                                                         | 1253        |
| 6.2.2.2 Ensure rsyslog service is enabled and active (Automated).....                                                                                         | 1255        |
| 6.2.2.3 Ensure all remote access methods are monitored (Automated) .....                                                                                      | 1257        |
| 6.2.2.4 Ensure journald is configured to send logs to rsyslog (Automated) .....                                                                               | 1261        |
| 6.2.2.5 Ensure rsyslog log file creation mode is configured (Automated) .....                                                                                 | 1265        |
| 6.2.2.6 Ensure rsyslog logging is configured (Manual).....                                                                                                    | 1267        |
| 6.2.2.7 Ensure rsyslog is configured to send logs to a remote log host (Manual).....                                                                          | 1270        |
| 6.2.2.8 Ensure rsyslog is not configured to receive logs from a remote client (Automated) .....                                                               | 1273        |
| 6.2.2.9 Ensure logrotate is configured (Manual).....                                                                                                          | 1275        |
| 6.2.2.10 Ensure rsyslog is configured to log cron events (Automated) .....                                                                                    | 1277        |
| 6.2.2.11 Ensure the rsyslog service is enabled and active (Automated).....                                                                                    | 1279        |
| 6.2.2.12 Ensure the operating system has the packages required for encrypting offloaded<br>audit logs (Automated).....                                        | 1281        |
| 6.2.2.13 Ensure the operating system authenticates the remote logging server for off-loading<br>audit logs (Automated).....                                   | 1283        |
| 6.2.2.14 Ensure the operating system encrypts audit records off-loaded onto a different<br>system or media from the system being audited (Automated) .....    | 1285        |
| 6.2.2.15 Ensure the audit system off-loads audit records onto a different system or media from<br>the system being audited (Automated) .....                  | 1288        |
| <b>6.2.3 Configure Logfiles</b> .....                                                                                                                         | <b>1290</b> |
| 6.2.3.1 Ensure access to all logfiles has been configured (Automated).....                                                                                    | 1291        |
| 6.2.3.2 Ensure /var/log/messages mode is configured (Automated).....                                                                                          | 1297        |
| 6.2.3.3 Ensure /var/log/messages owner is configured (Automated).....                                                                                         | 1299        |
| 6.2.3.4 Ensure /var/log/messages group owner is configured (Automated).....                                                                                   | 1301        |
| 6.2.3.5 Ensure /var/log is mode is configured (Automated).....                                                                                                | 1303        |
| 6.2.3.6 Ensure /var/log owner is configured (Automated) .....                                                                                                 | 1305        |
| 6.2.3.7 Ensure /var/log group owner is configured (Automated) .....                                                                                           | 1307        |
| 6.2.3.8 Ensure administrators are notified if an audit processing failure occurs by modifying<br>/etc/aliases (Automated) .....                               | 1309        |
| <b>6.3 System Auditing</b> .....                                                                                                                              | <b>1311</b> |
| <b>6.3.1 Configure auditd Service</b> .....                                                                                                                   | <b>1313</b> |
| 6.3.1.1 Ensure auditd packages are installed (Automated).....                                                                                                 | 1314        |
| 6.3.1.2 Ensure auditing for processes that start prior to auditd is enabled (Automated) .....                                                                 | 1316        |
| 6.3.1.3 Ensure audit_backlog_limit is sufficient (Automated) .....                                                                                            | 1320        |
| 6.3.1.4 Ensure auditd service is enabled and active (Automated) .....                                                                                         | 1324        |
| 6.3.1.5 Ensure the operating system allocates a sufficient audit_backlog_limit to capture<br>processes that start prior to the audit daemon (Automated) ..... | 1326        |
| 6.3.1.6 Ensure the operating system's audit daemon is configured to include local events<br>(Automated) .....                                                 | 1328        |
| 6.3.1.7 Ensure the operating system's audit daemon is configured to label all off-loaded audit<br>logs (Automated).....                                       | 1330        |
| 6.3.1.8 Ensure the operating system's audit daemon is configured to resolve audit information<br>before writing to disk (Automated) .....                     | 1332        |
| <b>6.3.2 Configure Data Retention</b> .....                                                                                                                   | <b>1334</b> |
| 6.3.2.1 Ensure audit log storage size is configured (Automated).....                                                                                          | 1335        |
| 6.3.2.2 Ensure audit logs are not automatically deleted (Automated).....                                                                                      | 1337        |
| 6.3.2.3 Ensure system is disabled when audit logs are full (Automated).....                                                                                   | 1339        |
| 6.3.2.4 Ensure system warns when audit logs are low on space (Automated).....                                                                                 | 1343        |
| 6.3.2.5 Ensure the operating system allocates audit record storage capacity (Manual) .....                                                                    | 1346        |

|                                                                                                                                                                                          |             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| 6.3.2.6 Ensure the SA and ISSO are notified in the event of an audit processing failure (Automated) .....                                                                                | 1349        |
| 6.3.2.7 Ensure the operating system notifies the SA and ISSO when allocated audit record storage volume reaches 75 percent (Automated) .....                                             | 1351        |
| 6.3.2.8 Ensure the operating system takes action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity (Automated) ..... | 1353        |
| 6.3.2.9 Ensure the audit system is configured to take an appropriate action when the internal event queue is full (Automated) .....                                                      | 1355        |
| <b>6.3.3 Configure auditd Rules .....</b>                                                                                                                                                | <b>1357</b> |
| 6.3.3.1 Ensure changes to system administration scope (sudoers) is collected (Automated) .....                                                                                           | 1358        |
| 6.3.3.2 Ensure actions as another user are always logged (Automated) .....                                                                                                               | 1362        |
| 6.3.3.3 Ensure events that modify the sudo log file are collected (Automated) .....                                                                                                      | 1366        |
| 6.3.3.4 Ensure events that modify date and time information are collected (Automated) ....                                                                                               | 1370        |
| 6.3.3.5 Ensure events that modify the system's network environment are collected (Automated) .....                                                                                       | 1374        |
| 6.3.3.6 Ensure use of privileged commands are collected (Automated) .....                                                                                                                | 1379        |
| 6.3.3.7 Ensure unsuccessful file access attempts are collected (Automated) .....                                                                                                         | 1383        |
| 6.3.3.8 Ensure events that modify user/group information are collected (Automated) .....                                                                                                 | 1387        |
| 6.3.3.9 Ensure discretionary access control permission modification events are collected (Automated) .....                                                                               | 1392        |
| 6.3.3.10 Ensure successful file system mounts are collected (Automated) .....                                                                                                            | 1398        |
| 6.3.3.11 Ensure session initiation information is collected (Automated) .....                                                                                                            | 1402        |
| 6.3.3.12 Ensure login and logout events are collected (Automated) .....                                                                                                                  | 1406        |
| 6.3.3.13 Ensure file deletion events by users are collected (Automated) .....                                                                                                            | 1410        |
| 6.3.3.14 Ensure events that modify the system's Mandatory Access Controls are collected (Automated) .....                                                                                | 1414        |
| 6.3.3.15 Ensure successful and unsuccessful attempts to use the chcon command are collected (Automated) .....                                                                            | 1417        |
| 6.3.3.16 Ensure successful and unsuccessful attempts to use the setfacl command are collected (Automated) .....                                                                          | 1421        |
| 6.3.3.17 Ensure successful and unsuccessful attempts to use the chacl command are collected (Automated) .....                                                                            | 1425        |
| 6.3.3.18 Ensure successful and unsuccessful attempts to use the usermod command are collected (Automated) .....                                                                          | 1429        |
| 6.3.3.19 Ensure kernel module loading unloading and modification is collected (Automated) .....                                                                                          | 1433        |
| 6.3.3.20 Ensure the audit configuration is immutable (Automated) .....                                                                                                                   | 1439        |
| 6.3.3.21 Ensure the running and on disk configuration is the same (Manual) .....                                                                                                         | 1442        |
| 6.3.3.22 Ensure successful and unsuccessful attempts to use the su command are collected (Automated) .....                                                                               | 1444        |
| 6.3.3.23 Ensure successful and unsuccessful attempts to use the sudo command are collected (Automated) .....                                                                             | 1447        |
| 6.3.3.24 Ensure successful and unsuccessful attempts to use the chsh command are collected (Automated) .....                                                                             | 1450        |
| 6.3.3.25 Ensure successful and unsuccessful attempts to use the crontab command are collected (Automated) .....                                                                          | 1453        |
| 6.3.3.26 Ensure successful and unsuccessful attempts to use the gpasswd command are collected (Automated) .....                                                                          | 1456        |
| 6.3.3.27 Ensure successful and unsuccessful attempts to use the newgrp command are collected (Automated) .....                                                                           | 1459        |
| 6.3.3.28 Ensure successful and unsuccessful attempts to use the pam_timestamp_check command are collected (Automated) .....                                                              | 1462        |
| 6.3.3.29 Ensure successful and unsuccessful attempts to use the ssh-keysign command are collected (Automated) .....                                                                      | 1465        |

|                                                                                                                     |             |
|---------------------------------------------------------------------------------------------------------------------|-------------|
| 6.3.3.30 Ensure successful and unsuccessful attempts to use the unix_chkpwd command are collected (Automated) ..... | 1468        |
| 6.3.3.31 Ensure successful and unsuccessful attempts to use the setsebool command are collected (Automated) .....   | 1471        |
| 6.3.3.32 Ensure successful and unsuccessful attempts to use the userhelper command are collected (Automated) .....  | 1474        |
| 6.3.3.33 Ensure successful and unsuccessful attempts to use the setfiles command are collected (Automated) .....    | 1477        |
| 6.3.3.34 Ensure successful and unsuccessful attempts to use the semanage command are collected (Automated) .....    | 1480        |
| 6.3.3.35 Ensure successful and unsuccessful attempts to use the postqueue command are collected (Automated) .....   | 1483        |
| 6.3.3.36 Ensure successful and unsuccessful attempts to use the postdrop command are collected (Automated) .....    | 1486        |
| 6.3.3.37 Ensure successful and unsuccessful attempts to use the unix_update command are collected (Automated) ..... | 1489        |
| 6.3.3.38 Ensure successful and unsuccessful attempts to use the umount command are collected (Automated) .....      | 1492        |
| 6.3.3.39 Ensure successful and unsuccessful attempts to use the mount command are collected (Automated) .....       | 1495        |
| 6.3.3.40 Ensure successful and unsuccessful attempts to use the ssh-agent command are collected (Automated) .....   | 1498        |
| 6.3.3.41 Ensure successful and unsuccessful attempts to use the passwd command are collected (Automated) .....      | 1501        |
| 6.3.3.42 Ensure successful and unsuccessful attempts to use the chage command are collected (Automated) .....       | 1504        |
| 6.3.3.43 Ensure the audit system prevents unauthorized changes to logon UIDs (Automated) .....                      | 1507        |
| 6.3.3.44 Ensure successful and unsuccessful modifications to the faillock file are collected (Automated) .....      | 1509        |
| <b>6.3.4 Configure auditd File Access .....</b>                                                                     | <b>1512</b> |
| 6.3.4.1 Ensure the audit log file directory mode is configured (Automated) .....                                    | 1513        |
| 6.3.4.2 Ensure audit log files mode is configured (Automated) .....                                                 | 1516        |
| 6.3.4.3 Ensure audit log files owner is configured (Automated) .....                                                | 1519        |
| 6.3.4.4 Ensure audit log files group owner is configured (Automated) .....                                          | 1522        |
| 6.3.4.5 Ensure audit configuration files mode is configured (Automated) .....                                       | 1525        |
| 6.3.4.6 Ensure audit configuration files owner is configured (Automated) .....                                      | 1528        |
| 6.3.4.7 Ensure audit configuration files group owner is configured (Automated) .....                                | 1530        |
| 6.3.4.8 Ensure audit tools mode is configured (Automated) .....                                                     | 1532        |
| 6.3.4.9 Ensure audit tools owner is configured (Automated) .....                                                    | 1535        |
| 6.3.4.10 Ensure audit tools group owner is configured (Automated) .....                                             | 1537        |
| 6.3.4.11 Ensure the audit logs are group-owned by root (Automated) .....                                            | 1539        |
| 6.3.4.12 Ensure audit tools are mode 0755 or more restrictive (Automated) .....                                     | 1541        |
| 6.3.4.13 Ensure the audit tools are owned by root (Automated) .....                                                 | 1543        |
| 6.3.4.14 Ensure audit tools are group owned by root (Automated) .....                                               | 1545        |
| 6.3.4.15 Ensure the audit log file directories are mode 0700 or more restrictive (Automated) .....                  | 1547        |
| 6.3.4.16 Ensure the audit log file directory is owned by root (Automated) .....                                     | 1549        |
| 6.3.4.17 Ensure audit log files group owner is root (Automated) .....                                               | 1551        |
| 6.3.4.18 Ensure audit log files are mode 0600 or more restrictive (Automated) .....                                 | 1553        |
| <b>7 System Maintenance .....</b>                                                                                   | <b>1555</b> |
| <b>7.1 System File Permissions .....</b>                                                                            | <b>1556</b> |
| 7.1.1 Ensure permissions on /etc/passwd are configured (Automated) .....                                            | 1557        |
| 7.1.2 Ensure permissions on /etc/passwd- are configured (Automated) .....                                           | 1559        |
| 7.1.3 Ensure permissions on /etc/group are configured (Automated) .....                                             | 1561        |

|                                                                                                                                                                |             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| 7.1.4 Ensure permissions on /etc/group- are configured (Automated).....                                                                                        | 1563        |
| 7.1.5 Ensure permissions on /etc/shadow are configured (Automated).....                                                                                        | 1565        |
| 7.1.6 Ensure permissions on /etc/shadow- are configured (Automated).....                                                                                       | 1567        |
| 7.1.7 Ensure permissions on /etc/gshadow are configured (Automated).....                                                                                       | 1569        |
| 7.1.8 Ensure permissions on /etc/gshadow- are configured (Automated).....                                                                                      | 1571        |
| 7.1.9 Ensure permissions on /etc/shells are configured (Automated) .....                                                                                       | 1573        |
| 7.1.10 Ensure permissions on /etc/security/opasswd are configured (Automated) .....                                                                            | 1575        |
| 7.1.11 Ensure world writable files and directories are secured (Automated) .....                                                                               | 1577        |
| 7.1.12 Ensure no files or directories without an owner and a group exist (Automated) .....                                                                     | 1581        |
| 7.1.13 Ensure SUID and SGID files are reviewed (Manual).....                                                                                                   | 1584        |
| 7.1.14 Ensure there are no ".shosts" files on the operating system (Automated).....                                                                            | 1587        |
| 7.1.15 Ensure there are no "shosts.equiv" files on the operating system (Automated) .....                                                                      | 1589        |
| 7.1.16 Ensure system-wide shared library directories have mode 755 or less permissive (Automated) .....                                                        | 1591        |
| 7.1.17 Ensure system-wide shared library directories must be owned by root (Automated).....                                                                    | 1593        |
| 7.1.18 Ensure the system-wide shared library directories are group-owned by root or a system account (Automated).....                                          | 1595        |
| 7.1.19 Ensure world-writable directories owner is configured (Manual).....                                                                                     | 1597        |
| 7.1.20 Ensure world-writable directories group-owner is configured (Manual) .....                                                                              | 1599        |
| 7.1.21 Ensure local initialization files do not execute world-writable programs (Manual) ....                                                                  | 1601        |
| 7.1.22 Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are mode 0755 or more restrictive (Automated) .....             | 1603        |
| 7.1.23 Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are owned by root (Automated) .....                             | 1605        |
| 7.1.24 Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are group-owned by root (Automated).....                        | 1607        |
| 7.1.25 Ensure the system-wide shared library files are mode 0755 or more restrictive (Automated) .....                                                         | 1609        |
| 7.1.26 Ensure the system-wide shared library files are owned by root (Automated) .....                                                                         | 1611        |
| 7.1.27 Ensure the system-wide shared library files are group-owned by root (Automated).....                                                                    | 1613        |
| <b>7.2 Local User and Group Settings .....</b>                                                                                                                 | <b>1615</b> |
| 7.2.1 Ensure accounts in /etc/passwd use shadowed passwords (Automated) .....                                                                                  | 1616        |
| 7.2.2 Ensure /etc/shadow password fields are not empty (Automated) .....                                                                                       | 1619        |
| 7.2.3 Ensure all groups in /etc/passwd exist in /etc/group (Automated).....                                                                                    | 1621        |
| 7.2.4 Ensure shadow group is empty (Automated) .....                                                                                                           | 1623        |
| 7.2.5 Ensure no duplicate UIDs exist (Automated).....                                                                                                          | 1625        |
| 7.2.6 Ensure no duplicate GIDs exist (Automated) .....                                                                                                         | 1627        |
| 7.2.7 Ensure no duplicate user names exist (Automated).....                                                                                                    | 1629        |
| 7.2.8 Ensure no duplicate group names exist (Automated).....                                                                                                   | 1631        |
| 7.2.9 Ensure local interactive user home directories are configured (Automated).....                                                                           | 1633        |
| 7.2.10 Ensure local interactive user dot files access is configured (Automated) .....                                                                          | 1638        |
| 7.2.11 Ensure all files and directories in the local interactive user home directory are group-owned by a group that the user is a member of (Automated) ..... | 1644        |
| 7.2.12 Ensure all files and directories in a local interactive user home directory are mode 0750 or more restrictive (Automated) .....                         | 1646        |
| 7.2.13 Ensure all local initialization files are mode 0740 or more restrictive (Automated) ...                                                                 | 1648        |
| 7.2.14 Ensure local interactive user home directories group-owner is their primary GID (Automated) .....                                                       | 1650        |
| 7.2.15 Ensure file executable search path statements do not share sensitive home directory information (Manual).....                                           | 1652        |
| <b>Appendix: Summary Table .....</b>                                                                                                                           | <b>1654</b> |
| <b>Appendix: CIS Controls v7 IG 1 Mapped Recommendations .....</b>                                                                                             | <b>1695</b> |
| <b>Appendix: CIS Controls v7 IG 2 Mapped Recommendations .....</b>                                                                                             | <b>1706</b> |

|                                                                           |                    |
|---------------------------------------------------------------------------|--------------------|
| <b><i>Appendix: CIS Controls v7 IG 3 Mapped Recommendations .....</i></b> | <b><i>1727</i></b> |
| <b><i>Appendix: CIS Controls v7 Unmapped Recommendations.....</i></b>     | <b><i>1748</i></b> |
| <b><i>Appendix: CIS Controls v8 IG 1 Mapped Recommendations .....</i></b> | <b><i>1750</i></b> |
| <b><i>Appendix: CIS Controls v8 IG 2 Mapped Recommendations .....</i></b> | <b><i>1763</i></b> |
| <b><i>Appendix: CIS Controls v8 IG 3 Mapped Recommendations .....</i></b> | <b><i>1784</i></b> |
| <b><i>Appendix: CIS Controls v8 Unmapped Recommendations.....</i></b>     | <b><i>1805</i></b> |
| <b><i>Appendix: Change History .....</i></b>                              | <b><i>1807</i></b> |

# Overview

All CIS Benchmarks™ (Benchmarks) focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the Benchmarks are designed to be a key **component** of a comprehensive cybersecurity program.

## Important Usage Information

All Benchmarks are available free for non-commercial use from the [CIS Website](#). They can be used to manually assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- [CIS Configuration Assessment Tool \(CIS-CAT® Pro Assessor\)](#)
- [CIS Benchmarks™ Certified 3rd Party Tooling](#)

These tools make the hardening process much more scalable for large numbers of systems and applications.

**NOTE:** Some tooling focuses only on the Benchmark Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that **ALL** Recommendations (**Automated** and **Manual**) be addressed since all are important for properly securing systems and are typically in scope for audits.

## Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

## Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To assure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.
- **Use the most recent version of a Benchmark:** This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

## Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.



## Remediation

CIS has developed [Build Kits](#) for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's "Remediation" section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

**When remediating systems (changing configuration settings on deployed systems as per the Benchmark's Recommendations), please approach this with caution and test thoroughly.**

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
  - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
  - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
  - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
  - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
  - When the initial deployment above is completed successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

## Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

**NOTE:** As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the [CIS Website](#). All other formats of the CIS Benchmarks™ (MS Word, Excel, and [Build Kits](#)) are available for CIS [SecureSuite®](#) members.

CIS-CAT® Pro is also available to CIS [SecureSuite®](#) members.

## Target Technology Details

This document provides prescriptive guidance for establishing a secure configuration posture for Red Hat Enterprise Linux 8 systems running on x86\_64 platforms.

This guide was developed and tested against Red Hat Enterprise Linux 8.10

The guidance within broadly assumes that operations are being performed as the **root** user, and executed under the default Bash version for the applicable distribution.

Operations performed using **sudo** instead of the **root** user, or executed under another shell, may produce unexpected results, or fail to make the intended changes to the system. Non-root users may not be able to access certain areas of the system, especially after remediation has been performed. It is advisable to verify **root** users path integrity and the integrity of any programs being run prior to execution of commands and scripts included in this benchmark.

The default prompt for the **root** user is **#**, and as such all sample commands will have **#** as an additional indication that it is to be executed as **root**.

To obtain the latest version of this guide, please visit <http://workbench.cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at [feedback@cisecurity.org](mailto:feedback@cisecurity.org).

## Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Red Hat Enterprise Linux 8 on x86\_64 platforms.

## Consensus Guidance

This CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.

## Typographical Conventions

The following typographical conventions are used throughout this guide:

| Convention                                      | Meaning                                                                                                                                                           |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>Stylized Monospace font</code>            | Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.                                                           |
| <code>Monospace font</code>                     | Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.                                                  |
| <code>&lt;Monospace font in brackets&gt;</code> | Text set in angle brackets denote a variable requiring substitution for a real value.                                                                             |
| <i>Italic font</i>                              | Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.  |
| <b>Bold font</b>                                | Additional information or caveats things like <b>Notes</b> , <b>Warnings</b> , or <b>Cautions</b> (usually just the word itself and the rest of the text normal). |

# Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

## Title

Concise description for the recommendation's intended configuration.

## Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

### Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

### Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

## Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

## Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

## Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

## **Impact Statement**

Any security, functionality, or operational consequences that can result from following the recommendation.

## **Audit Procedure**

Systematic instructions for determining if the target system complies with the recommendation.

## **Remediation Procedure**

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

## **Default Value**

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

## **References**

Additional documentation relative to the recommendation.

## **CIS Critical Security Controls® (CIS Controls®)**

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) "4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

## **Additional Information**

Supplementary information that does not correspond to any other field but may be useful to the user.

## Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - Server**

Items in this profile intend to:

- be practical and prudent;
- provide a clear security benefit; and
- not inhibit the utility of the technology beyond acceptable means.

This profile is intended for servers.

- **Level 2 - Server**

This profile extends the "Level 1 - Server" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

This profile is intended for servers.

- **Level 1 - Workstation**

Items in this profile intend to:

- be practical and prudent;
- provide a clear security benefit; and
- not inhibit the utility of the technology beyond acceptable means.

This profile is intended for workstations.

- **Level 2 - Workstation**

This profile extends the "Level 1 - Workstation" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

This profile is intended for workstations.

- **STIG**

Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where following STIG based security guidance is paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

This profile is intended for servers and workstations.

## Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

This benchmark is based upon previous Linux benchmarks published and would not be possible without the contributions provided over the history of all of these benchmarks. The CIS community thanks everyone who has contributed to the Linux benchmarks.

### **Contributor**

Eric Pinnell  
Ron Colvin  
Dave Billing  
Dominic Pace  
Koen Laevens  
Mark Birch  
Thomas Sjögren  
James Trigg  
Matthew Burket  
Marcus Burghardt  
Graham Eames  
Robert McSulla  
Chad Streck  
Ryan Jaynes  
Tamas Tevesz  
Gokhan Lus  
Cory Sherman  
Simon John

### **Editor**

Jonathan Lewis Christopherson  
Eric Pinnell  
Justin Brown  
Randie Bejar



# Recommendations

## 1 Initial Setup

Items in this section are advised for all systems, but may be difficult or require extensive preparation after the initial setup of the system.

## 1.1 Filesystem

The file system is generally a built-in layer used to handle the data management of the storage.

### 1.1.1 Configure Filesystem Kernel Modules

Several uncommon filesystem types are supported under Linux. Removing support for unneeded filesystem types reduces the local attack surface of the system. If a filesystem type is not needed it should be disabled. Native Linux file systems are designed to ensure that built-in security controls function as expected. Non-native filesystems can lead to unexpected consequences to both the security and functionality of the system and should be used with caution. Many filesystems are created for niche use cases and are not maintained and supported as the operating systems are updated and patched. Users of non-native filesystems should ensure that there is attention and ongoing support for them, especially in light of frequent operating system changes.

Standard network connectivity and Internet access to cloud storage may make the use of non-standard filesystem formats to directly attach heterogeneous devices much less attractive.

**Note:** This should not be considered a comprehensive list of filesystems. You may wish to consider additions to those listed here for your environment. For the current available file system modules on the system see `/usr/lib/modules/$(uname -r)/kernel/fs`

#### Start up scripts

Kernel modules loaded directly via `insmod` will ignore what is configured in the relevant `/etc/modprobe.d/*.conf` files. If modules are still being loaded after a reboot whilst having the correctly configured `blacklist` and `install` command, check for `insmod` entries in start up scripts such as `.bashrc`.

You may also want to check `/lib/modprobe.d/`. Please note that this directory should not be used for user defined module loading. Ensure that all such entries resides in `/etc/modprobe.d/*.conf` files.

#### Return values

Using `/bin/false` as the command in disabling a particular module serves two purposes; to convey the meaning of the entry to the user and cause a non-zero return value. The latter can be tested for in scripts. Please note that `insmod` will ignore what is configured in the relevant `/etc/modprobe.d/*.conf` files. The preferred way to load modules is with `modprobe`.

### *1.1.1.1 Ensure cramfs kernel module is not available (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### **Description:**

The **cramfs** filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A **cramfs** image can be used without having to first decompress the image.

#### **Rationale:**

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

#### **Audit:**

Run the following script to verify:

- **IF** - the **cramfs** kernel module is available in ANY installed kernel, verify:

- An entry including **/bin/true** or **/bin/false** exists in a file within the **/etc/modprobe.d/** directory
- The module is deny listed in a file within the **/etc/modprobe.d/** directory
- The module is not loaded in the running kernel

- **IF** - the **cramfs** kernel module is not available on the system, or pre-compiled into the kernel, no additional configuration is necessary

```

#!/usr/bin/env bash

{
    a_output=() a_output2=() a_output3=() l_dl="" l_mod_name="cramfs"
    l_mod_type="fs"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_chk()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if ! lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loaded")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loaded")
            fi
            if grep -Pq -- '\bbinstall\h+'${l_mod_chk_name//-/}_
/_}'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loadable")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loadable")
            fi
            if grep -Pq -- '\bbblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is deny listed")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is not deny listed")
            fi
        }
        for l_mod_base_directory in $l_mod_path; do
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name:-2)"
                [ "$l_dl" != "y" ] && f_module_chk
            else
                a_output+=(" - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\"")
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        if [ "${#a_output2[@]}" -le 0 ]; then
            printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}"
        else
            printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
            [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "- Correctly set:"
"${a_output[@]}"
        fi
    }
}

```

## Remediation:

Run the following script to unload and disable the `cramfs` module:

- **IF** - the `cramfs` kernel module is available in ANY installed kernel:

- Create a file ending in `.conf` with `install cramfs /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist cramfs` in the `/etc/modprobe.d/` directory
- Run `modprobe -r cramfs 2>/dev/null; rmmod cramfs 2>/dev/null` to remove `cramfs` from the kernel

- **IF** - the `cramfs` kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

```

#!/usr/bin/env bash

{
    a_output2=() a_output3=() l_dl="" l_mod_name="cramfs" l_mod_type="fs"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_fix()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output2+=(" - unloading kernel module: \"$l_mod_name\"")
                modprobe -r "$l_mod_chk_name" 2>/dev/null; rmmod "$l_mod_name"
2>/dev/null
            fi
            if ! grep -Pq -- '\binstall\h+'${l_mod_chk_name//-/}_
/_'\b'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output2+=(" - setting kernel module: \"$l_mod_name\" to
\"$(readlink -f /bin/false)\"")
                printf '%s\n' "install $l_mod_chk_name $(readlink -f /bin/false)" >>
/etc/modprobe.d/"$l_mod_name".conf
            fi
            if ! grep -Pq -- '\bblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output2+=(" - denylisting kernel module: \"$l_mod_name\"")
                printf '%s\n' "blacklist $l_mod_chk_name" >>
/etc/modprobe.d/"$l_mod_name".conf
            fi
        }
        for l_mod_base_directory in $l_mod_path; do # Check if the module exists
on the system
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name:-2"
                [ "$l_dl" != "y" ] && f_module_fix
            else
                printf '%s\n' " - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\""
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        [ "${#a_output2[@]}" -gt 0 ] && printf '%s\n' "" "${a_output2[@]}" ||
printf '%s\n' "" " - No changes needed"
        printf '%s\n' "" " - remediation of kernel module: \"$l_mod_name\"
complete" ""
    }
}

```

## References:

1. NIST SP 800-53 Rev. 5: CM-7
2. STIG Finding ID: V-230498
3. NIST SP 800-53A :: CM-7.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230498  
Rule ID: SV-230498r942930  
STIG ID: RHEL-08-040025  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |    |    |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1005, T1005.000            | TA0005  | M1050       |



### *1.1.1.2 Ensure freevxfs kernel module is not available (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The **freevxfs** filesystem type is a free version of the Veritas type filesystem. This is the primary filesystem type for HP-UX operating systems.

#### **Rationale:**

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

#### **Audit:**

Run the following script to verify:

- **IF** - the **freevxfs** kernel module is available in ANY installed kernel, verify:

- An entry including **/bin/true** or **/bin/false** exists in a file within the **/etc/modprobe.d/** directory
- The module is deny listed in a file within the **/etc/modprobe.d/** directory
- The module is not loaded in the running kernel

- **IF** - the **freevxfs** kernel module is not available on the system, or pre-compiled into the kernel, no additional configuration is necessary

```

#!/usr/bin/env bash

{
    a_output=() a_output2=() a_output3=() l_dl="" l_mod_name="freevxfs"
    l_mod_type="fs"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_chk()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if ! lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loaded")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loaded")
            fi
            if grep -Pq -- '\bbinstall\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loadable")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loadable")
            fi
            if grep -Pq -- '\bbblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is deny listed")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is not deny listed")
            fi
        }
        for l_mod_base_directory in $l_mod_path; do
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name:-2"
                [ "$l_dl" != "y" ] && f_module_chk
            else
                a_output+=(" - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\"")
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        if [ "${#a_output2[@]}" -le 0 ]; then
            printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}"
        else
            printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
            [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "- Correctly set:"
"${a_output[@]}"
        fi
    }
}

```

## Remediation:

Run the following script to unload and disable the `freevxfs` module:

- **IF** - the `freevxfs` kernel module is available in ANY installed kernel:

- Create a file ending in `.conf` with `install freevxfs /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist freevxfs` in the `/etc/modprobe.d/` directory
- Run `modprobe -r freevxfs 2>/dev/null; rmmod freevxfs 2>/dev/null` to remove `freevxfs` from the kernel

- **IF** - the `freevxfs` kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

```
#!/usr/bin/env bash

{
  a_output2=() a_output3=() l_dl="" l_mod_name="freevxfs" l_mod_type="fs"
  l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
  f_module_fix()
  {
    l_dl="y" a_showconfig=()
    while IFS= read -r l_showconfig; do
      a_showconfig+=("$l_showconfig")
      done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
      if lsmod | grep "$l_mod_chk_name" &> /dev/null; then
        a_output2+=(" - unloading kernel module: \"$l_mod_name\"")
        modprobe -r "$l_mod_chk_name" 2>/dev/null; rmmod "$l_mod_name"
2>/dev/null
      fi
      if ! grep -Pq -- '\binstall\h+'${l_mod_chk_name//-/}_
/_'\b'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
        a_output2+=(" - setting kernel module: \"$l_mod_name\" to
\"$(readlink -f /bin/false)\"")
        printf '%s\n' "install $l_mod_chk_name $(readlink -f /bin/false)" >>
/etc/modprobe.d/"$l_mod_name".conf
      fi
      if ! grep -Pq -- '\bblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
        a_output2+=(" - denylisting kernel module: \"$l_mod_name\"")
        printf '%s\n' "blacklist $l_mod_chk_name" >>
/etc/modprobe.d/"$l_mod_name".conf
      fi
    }
    for l_mod_base_directory in $l_mod_path; do # Check if the module exists
on the system
      if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
        a_output3+=(" - \"$l_mod_base_directory\"")
        l_mod_chk_name="$l_mod_name"
        [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="${l_mod_name::-2}"
        [ "$l_dl" != "y" ] && f_module_fix
      else
        printf '%s\n' " - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\""
      fi
    done
    [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
    [ "${#a_output2[@]}" -gt 0 ] && printf '%s\n' "" "${a_output2[@]}" ||
printf '%s\n' "" " - No changes needed"
    printf '%s\n' "" " - remediation of kernel module: \"$l_mod_name\"
complete" ""
  }
}
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1005, T1005.000            | TA0005  | M1050       |

### *1.1.1.3 Ensure hfs kernel module is not available (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The **hfs** filesystem type is a hierarchical filesystem that allows you to mount Mac OS filesystems.

#### **Rationale:**

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

#### **Audit:**

Run the following script to verify:

- **IF** - the **hfs** kernel module is available in ANY installed kernel, verify:

- An entry including **/bin/true** or **/bin/false** exists in a file within the **/etc/modprobe.d/** directory
- The module is deny listed in a file within the **/etc/modprobe.d/** directory
- The module is not loaded in the running kernel

- **IF** - the **hfs** kernel module is not available on the system, or pre-compiled into the kernel, no additional configuration is necessary

```

#!/usr/bin/env bash

{
    a_output=() a_output2=() a_output3=() l_dl="" l_mod_name="hfs"
    l_mod_type="fs"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_chk()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if ! lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loaded")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loaded")
            fi
            if grep -Pq -- '\bbinstall\h+'${l_mod_chk_name//-/}_
/_}'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loadable")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loadable")
            fi
            if grep -Pq -- '\bbblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is deny listed")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is not deny listed")
            fi
        }
        for l_mod_base_directory in $l_mod_path; do
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name:-2"
                [ "$l_dl" != "y" ] && f_module_chk
            else
                a_output+=(" - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\"")
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        if [ "${#a_output2[@]}" -le 0 ]; then
            printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}"
        else
            printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
            [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "- Correctly set:"
"${a_output[@]}"
        fi
    }
}

```

## Remediation:

Run the following script to unload and disable the `hfs` module:

- **IF** - the `hfs` kernel module is available in ANY installed kernel:

- Create a file ending in `.conf` with `install hfs /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist hfs` in the `/etc/modprobe.d/` directory
- Run `modprobe -r hfs 2>/dev/null; rmmod hfs 2>/dev/null` to remove `hfs` from the kernel

- **IF** - the `hfs` kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary



```
#!/usr/bin/env bash

{
    a_output2=() a_output3=() l_dl="" l_mod_name="hfs" l_mod_type="fs"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_fix()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output2+=(" - unloading kernel module: \"$l_mod_name\"")
                modprobe -r "$l_mod_chk_name" 2>/dev/null; rmmod "$l_mod_name"
2>/dev/null
            fi
            if ! grep -Pq -- '\binstall\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output2+=(" - setting kernel module: \"$l_mod_name\" to
\"$(readlink -f /bin/false)\"")
                printf '%s\n' "install $l_mod_chk_name $(readlink -f /bin/false)" >>
/etc/modprobe.d/"$l_mod_name".conf
            fi
            if ! grep -Pq -- '\bblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output2+=(" - denylisting kernel module: \"$l_mod_name\"")
                printf '%s\n' "blacklist $l_mod_chk_name" >>
/etc/modprobe.d/"$l_mod_name".conf
            fi
        }
        for l_mod_base_directory in $l_mod_path; do # Check if the module exists
on the system
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name:-2"
                [ "$l_dl" != "y" ] && f_module_fix
            else
                printf '%s\n' " - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\""
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        [ "${#a_output2[@]}" -gt 0 ] && printf '%s\n' "" "${a_output2[@]}" ||
printf '%s\n' "" " - No changes needed"
        printf '%s\n' "" " - remediation of kernel module: \"$l_mod_name\"
complete" ""
    }
}
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1005, T1005.000            | TA0005  | M1050       |

### *1.1.1.4 Ensure hfsplus kernel module is not available (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The **hfsplus** filesystem type is a hierarchical filesystem designed to replace **hfs** that allows you to mount Mac OS filesystems.

#### **Rationale:**

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

#### **Audit:**

Run the following script to verify:

- **IF** - the **hfsplus** kernel module is available in ANY installed kernel, verify:

- An entry including **/bin/true** or **/bin/false** exists in a file within the **/etc/modprobe.d/** directory
- The module is deny listed in a file within the **/etc/modprobe.d/** directory
- The module is not loaded in the running kernel

- **IF** - the **hfsplus** kernel module is not available on the system, or pre-compiled into the kernel, no additional configuration is necessary

```

#!/usr/bin/env bash

{
    a_output=() a_output2=() a_output3=() l_dl="" l_mod_name="hfsplus"
    l_mod_type="fs"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_chk()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if ! lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loaded")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loaded")
            fi
            if grep -Pq -- '\bbinstall\h+'${l_mod_chk_name//-/}_
/_}'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loadable")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loadable")
            fi
            if grep -Pq -- '\bbblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is deny listed")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is not deny listed")
            fi
        }
        for l_mod_base_directory in $l_mod_path; do
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name:-2"
                [ "$l_dl" != "y" ] && f_module_chk
            else
                a_output+=(" - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\"")
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        if [ "${#a_output2[@]}" -le 0 ]; then
            printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}"
        else
            printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
            [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "- Correctly set:"
"${a_output[@]}"
        fi
    }
}

```

## Remediation:

Run the following script to unload and disable the `hfsplus` module:

- **IF** - the `hfsplus` kernel module is available in ANY installed kernel:

- Create a file ending in `.conf` with `install hfsplus /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist hfsplus` in the `/etc/modprobe.d/` directory
- Run `modprobe -r hfsplus 2>/dev/null; rmmod hfsplus 2>/dev/null` to remove `hfsplus` from the kernel

- **IF** - the `hfsplus` kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

```
#!/usr/bin/env bash

{
  a_output2=() a_output3=() l_dl="" l_mod_name="hfsplus" l_mod_type="fs"
  l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
  f_module_fix()
  {
    l_dl="y" a_showconfig=()
    while IFS= read -r l_showconfig; do
      a_showconfig+=("$l_showconfig")
      done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
      if lsmod | grep "$l_mod_chk_name" &> /dev/null; then
        a_output2+=(" - unloading kernel module: \"$l_mod_name\"")
        modprobe -r "$l_mod_chk_name" 2>/dev/null; rmmod "$l_mod_name"
2>/dev/null
      fi
      if ! grep -Pq -- '\binstall\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
        a_output2+=(" - setting kernel module: \"$l_mod_name\" to
\"$(readlink -f /bin/false)\"")
        printf '%s\n' "install $l_mod_chk_name $(readlink -f /bin/false)" >>
/etc/modprobe.d/"$l_mod_name".conf
      fi
      if ! grep -Pq -- '\bblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
        a_output2+=(" - denylisting kernel module: \"$l_mod_name\"")
        printf '%s\n' "blacklist $l_mod_chk_name" >>
/etc/modprobe.d/"$l_mod_name".conf
      fi
    }
    for l_mod_base_directory in $l_mod_path; do # Check if the module exists
on the system
      if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
        a_output3+=(" - \"$l_mod_base_directory\"")
        l_mod_chk_name="$l_mod_name"
        [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="${l_mod_name::-2}"
        [ "$l_dl" != "y" ] && f_module_fix
      else
        printf '%s\n' " - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\""
      fi
    done
    [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
    [ "${#a_output2[@]}" -gt 0 ] && printf '%s\n' "" "${a_output2[@]}" ||
printf '%s\n' "" " - No changes needed"
    printf '%s\n' "" " - remediation of kernel module: \"$l_mod_name\"
complete" ""
  }
}
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1005, T1005.000            | TA0005  | M1050       |

### *1.1.1.5 Ensure jffs2 kernel module is not available (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The **jffs2** (journaling flash filesystem 2) filesystem type is a log-structured filesystem used in flash memory devices.

#### **Rationale:**

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

#### **Audit:**

Run the following script to verify:

- **IF** - the **jffs2** kernel module is available in ANY installed kernel, verify:

- An entry including **/bin/true** or **/bin/false** exists in a file within the **/etc/modprobe.d/** directory
- The module is deny listed in a file within the **/etc/modprobe.d/** directory
- The module is not loaded in the running kernel

- **IF** - the **jffs2** kernel module is not available on the system, or pre-compiled into the kernel, no additional configuration is necessary



```

#!/usr/bin/env bash

{
    a_output=() a_output2=() a_output3=() l_dl="" l_mod_name="jffs2"
    l_mod_type="fs"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_chk()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if ! lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loaded")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loaded")
            fi
            if grep -Pq -- '\bbinstall\h+'${l_mod_chk_name//-/}_
/_}'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loadable")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loadable")
            fi
            if grep -Pq -- '\bbblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is deny listed")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is not deny listed")
            fi
        }
        for l_mod_base_directory in $l_mod_path; do
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name:-2"
                [ "$l_dl" != "y" ] && f_module_chk
            else
                a_output+=(" - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\"")
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        if [ "${#a_output2[@]}" -le 0 ]; then
            printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}"
        else
            printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
            [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "- Correctly set:"
"${a_output[@]}"
        fi
    }
}

```

## Remediation:

Run the following script to unload and disable the `jffs2` module:

- **IF** - the `jffs2` kernel module is available in ANY installed kernel:

- Create a file ending in `.conf` with `install jffs2 /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist jffs2` in the `/etc/modprobe.d/` directory
- Run `modprobe -r jffs2 2>/dev/null; rmmod jffs2 2>/dev/null` to remove `jffs2` from the kernel

- **IF** - the `jffs2` kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

```
#!/usr/bin/env bash

{
    a_output2=() a_output3=() l_dl="" l_mod_name="jffs2" l_mod_type="fs"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_fix()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output2+=(" - unloading kernel module: \"$l_mod_name\"")
                modprobe -r "$l_mod_chk_name" 2>/dev/null; rmmod "$l_mod_name"
2>/dev/null
            fi
            if ! grep -Pq -- '\binstall\h+'${l_mod_chk_name//-/}_
/_'\b'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output2+=(" - setting kernel module: \"$l_mod_name\" to
\"$(readlink -f /bin/false)\"")
                printf '%s\n' "install $l_mod_chk_name $(readlink -f /bin/false)" >>
/etc/modprobe.d/"$l_mod_name".conf
            fi
            if ! grep -Pq -- '\bblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output2+=(" - denylisting kernel module: \"$l_mod_name\"")
                printf '%s\n' "blacklist $l_mod_chk_name" >>
/etc/modprobe.d/"$l_mod_name".conf
            fi
        }
        for l_mod_base_directory in $l_mod_path; do # Check if the module exists
on the system
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name:-2"
                [ "$l_dl" != "y" ] && f_module_fix
            else
                printf '%s\n' " - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\""
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        [ "${#a_output2[@]}" -gt 0 ] && printf '%s\n' "" "${a_output2[@]}" ||
printf '%s\n' "" " - No changes needed"
        printf '%s\n' "" " - remediation of kernel module: \"$l_mod_name\"
complete" ""
    }
}
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1005, T1005.000            | TA0005  | M1050       |

### 1.1.1.6 Ensure overlayfs kernel module is not available (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

#### Description:

**overlayfs** is a Linux filesystem that layers multiple filesystems to create a single unified view which allows a user to "merge" several mount points into a unified filesystem.

#### Rationale:

The **overlayfs** has known CVE's: CVE-2023-32629, CVE-2023-2640, CVE-2023-0386. Disabling the **overlayfs** reduces the local attack surface by removing support for unnecessary filesystem types and mitigates potential risks associated with unauthorized execution of setuid files, enhancing the overall system security.

#### Impact:

**WARNING: If Container applications such as Docker, Kubernetes, Podman, Linux Containers (LXC), etc. are in use proceed with caution and consider the impact on containerized workloads, as disabling the **overlayfs** may severely disrupt containerization.**

#### Audit:

Run the following script to verify:

- **IF** - the **overlayfs** kernel module is available in ANY installed kernel, verify:

- An entry including **/bin/true** or **/bin/false** exists in a file within the **/etc/modprobe.d/** directory
- The module is deny listed in a file within the **/etc/modprobe.d/** directory
- The module is not loaded in the running kernel

- **IF** - the **overlayfs** kernel module is not available on the system, or pre-compiled into the kernel, no additional configuration is necessary

```

#!/usr/bin/env bash

{
    a_output=() a_output2=() a_output3=() l_dl="" l_mod_name="overlayfs"
    l_mod_type="fs"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_chk()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if ! lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loaded")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loaded")
            fi
            if grep -Pq -- '\binstall\h+'${l_mod_chk_name//-/}_
/_}'\h+(\usr)?\bin\(/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loadable")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loadable")
            fi
            if grep -Pq -- '\bblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is deny listed")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is not deny listed")
            fi
        }
        for l_mod_base_directory in $l_mod_path; do
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name:-2)"
                [ "$l_dl" != "y" ] && f_module_chk
            else
                a_output+=(" - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\"")
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        if [ "${#a_output2[@]}" -le 0 ]; then
            printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}"
        else
            printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
            [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "- Correctly set:"
"${a_output[@]}"
        fi
    }
}

```

## Remediation:

Run the following script to unload and disable the `overlayfs` module:

- **IF** - the `overlayfs` kernel module is available in ANY installed kernel:

- Create a file ending in `.conf` with `install overlayfs /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist overlayfs` in the `/etc/modprobe.d/` directory
- Run `modprobe -r overlay 2>/dev/null; rmmod overlay 2>/dev/null` to remove `overlayfs` from the kernel

- **IF** - the `overlayfs` kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

```

#!/usr/bin/env bash

{
    a_output2=() a_output3=() l_dl="" l_mod_name="overlayfs" l_mod_type="fs"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_fix()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output2+=(" - unloading kernel module: \"$l_mod_name\"")
                modprobe -r "$l_mod_chk_name" 2>/dev/null; rmmod "$l_mod_name"
2>/dev/null
            fi
            if ! grep -Pq -- '\binstall\h+'${l_mod_chk_name//-/}_
/_'\b'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output2+=(" - setting kernel module: \"$l_mod_name\" to
\"$(readlink -f /bin/false)\"")
                printf '%s\n' "install $l_mod_chk_name $(readlink -f /bin/false)" >>
/etc/modprobe.d/"$l_mod_name".conf
            fi
            if ! grep -Pq -- '\bblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output2+=(" - denylisting kernel module: \"$l_mod_name\"")
                printf '%s\n' "blacklist $l_mod_chk_name" >>
/etc/modprobe.d/"$l_mod_name".conf
            fi
        }
        for l_mod_base_directory in $l_mod_path; do # Check if the module exists
on the system
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="${l_mod_name::-2}"
                [ "$l_dl" != "y" ] && f_module_fix
            else
                printf '%s\n' " - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\""
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        [ "${#a_output2[@]}" -gt 0 ] && printf '%s\n' "" "${a_output2[@]}" ||
printf '%s\n' "" " - No changes needed"
        printf '%s\n' "" " - remediation of kernel module: \"$l_mod_name\"
complete" ""
    }
}

```



## References:

1. NIST SP 800-53 Rev. 5: CM-7
2. <https://docs.kernel.org/filesystems/overlayfs.html>
3. [https://wiki.archlinux.org/title/Overlay\\_filesystem](https://wiki.archlinux.org/title/Overlay_filesystem)
4. <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=overlayfs>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1005, T1005.000            | TA0005  | M1050       |

### 1.1.1.7 Ensure squashfs kernel module is not available (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

#### Description:

The **squashfs** filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A **squashfs** image can be used without having to first decompress the image.

#### Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

#### Impact:

As Snap packages utilize **squashfs** as a compressed filesystem, disabling **squashfs** will cause Snap packages to fail.

**Snap** application packages of software are self-contained and work across a range of Linux distributions. This is unlike traditional Linux package management approaches, like APT or RPM, which require specifically adapted packages per Linux distribution on an application update and delay therefore application deployment from developers to their software's end-user. Snaps themselves have no dependency on any external store ("App store"), can be obtained from any source and can be therefore used for upstream software deployment.

#### Audit:

Run the following script to verify:

- **IF** - the **squashfs** kernel module is available in ANY installed kernel, verify:

- An entry including **/bin/true** or **/bin/false** exists in a file within the **/etc/modprobe.d/** directory
- The module is deny listed in a file within the **/etc/modprobe.d/** directory
- The module is not loaded in the running kernel

- **IF** - the **squashfs** kernel module is not available on the system, or pre-compiled into the kernel, no additional configuration is necessary

```

#!/usr/bin/env bash

{
    a_output=() a_output2=() a_output3=() l_dl="" l_mod_name="squashfs"
    l_mod_type="fs"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_chk()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if ! lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loaded")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loaded")
            fi
            if grep -Pq -- '\bbinstall\h+'${l_mod_chk_name//-/}_
/_}'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loadable")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loadable")
            fi
            if grep -Pq -- '\bbblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is deny listed")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is not deny listed")
            fi
        }
        for l_mod_base_directory in $l_mod_path; do
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name:-2"
                [ "$l_dl" != "y" ] && f_module_chk
            else
                a_output+=(" - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\"")
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        if [ "${#a_output2[@]}" -le 0 ]; then
            printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}"
        else
            printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
            [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "- Correctly set:"
"${a_output[@]}"
        fi
    }
}

```

**Note:** On operating systems where `squashfs` is pre-build into the kernel:

- This is considered an acceptable "passing" state
- The kernel **should not** be re-compiled to remove `squashfs`
- This audit will return a passing state with "module: "squashfs" doesn't exist in ..."

### Remediation:

Run the following script to unload and disable the `udf` module:

- **IF** - the `squashfs` kernel module is available in ANY installed kernel:

- Create a file ending in `.conf` with `install squashfs /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist squashfs` in the `/etc/modprobe.d/` directory
- Run `modprobe -r squashfs 2>/dev/null; rmmod squashfs 2>/dev/null` to remove `squashfs` from the kernel

- **IF** - the `squashfs` kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

```
#!/usr/bin/env bash

{
  a_output2=() a_output3=() l_dl="" l_mod_name="squashfs" l_mod_type="fs"
  l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
  f_module_fix()
  {
    l_dl="y" a_showconfig=()
    while IFS= read -r l_showconfig; do
      a_showconfig+=("$l_showconfig")
      done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
      if lsmod | grep "$l_mod_chk_name" &> /dev/null; then
        a_output2+=(" - unloading kernel module: \"$l_mod_name\"")
        modprobe -r "$l_mod_chk_name" 2>/dev/null; rmmod "$l_mod_name"
2>/dev/null
      fi
      if ! grep -Pq -- '\binstall\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
        a_output2+=(" - setting kernel module: \"$l_mod_name\" to
\"$(readlink -f /bin/false)\"")
        printf '%s\n' "install $l_mod_chk_name $(readlink -f /bin/false)" >>
/etc/modprobe.d/"$l_mod_name".conf
      fi
      if ! grep -Pq -- '\bblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
        a_output2+=(" - denylisting kernel module: \"$l_mod_name\"")
        printf '%s\n' "blacklist $l_mod_chk_name" >>
/etc/modprobe.d/"$l_mod_name".conf
      fi
    }
    for l_mod_base_directory in $l_mod_path; do # Check if the module exists
on the system
      if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
        a_output3+=(" - \"$l_mod_base_directory\"")
        l_mod_chk_name="$l_mod_name"
        [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="${l_mod_name::-2}"
        [ "$l_dl" != "y" ] && f_module_fix
      else
        printf '%s\n' " - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\""
      fi
    done
    [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
    [ "${#a_output2[@]}" -gt 0 ] && printf '%s\n' "" "${a_output2[@]}" ||
printf '%s\n' "" " - No changes needed"
    printf '%s\n' "" " - remediation of kernel module: \"$l_mod_name\"
complete" ""
  }
}
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1005, T1005.000            | TA0005  | M1050       |

### *1.1.1.8 Ensure udf kernel module is not available (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

The **udf** filesystem type is the universal disk format used to implement ISO/IEC 13346 and ECMA-167 specifications. This is an open vendor filesystem type for data storage on a broad range of media. This filesystem type is necessary to support writing DVDs and newer optical disc formats.

#### **Rationale:**

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

#### **Impact:**

Microsoft Azure requires the usage of **udf**.

**udf should not** be disabled on systems run on Microsoft Azure.

#### **Audit:**

Run the following script to verify:

- **IF** - the **udf** kernel module is available in ANY installed kernel, verify:

- An entry including **/bin/true** or **/bin/false** exists in a file within the **/etc/modprobe.d/** directory
- The module is deny listed in a file within the **/etc/modprobe.d/** directory
- The module is not loaded in the running kernel

- **IF** - the **udf** kernel module is not available on the system, or pre-compiled into the kernel, no additional configuration is necessary

```

#!/usr/bin/env bash

{
    a_output=() a_output2=() a_output3=() l_dl="" l_mod_name="udf"
    l_mod_type="fs"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_chk()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if ! lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loaded")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loaded")
            fi
            if grep -Pq -- '\bbinstall\h+'${l_mod_chk_name//-/}_
/_}'\h+(\usr)?\bin\(/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loadable")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loadable")
            fi
            if grep -Pq -- '\bbblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is deny listed")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is not deny listed")
            fi
        }
        for l_mod_base_directory in $l_mod_path; do
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name:-2)"
                [ "$l_dl" != "y" ] && f_module_chk
            else
                a_output+=(" - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\"")
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        if [ "${#a_output2[@]}" -le 0 ]; then
            printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}"
        else
            printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
            [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "- Correctly set:"
"${a_output[@]}"
        fi
    }
}

```



## Remediation:

Run the following script to unload and disable the `udf` module:

- **IF** - the `udf` kernel module is available in ANY installed kernel:

- Create a file ending in `.conf` with `install udf /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist udf` in the `/etc/modprobe.d/` directory
- Run `modprobe -r udf 2>/dev/null; rmmod udf 2>/dev/null` to remove `udf` from the kernel

- **IF** - the `udf` kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

```
#!/usr/bin/env bash

{
  a_output2=() a_output3=() l_dl="" l_mod_name="udf" l_mod_type="fs"
  l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
  f_module_fix()
  {
    l_dl="y" a_showconfig=()
    while IFS= read -r l_showconfig; do
      a_showconfig+=("$l_showconfig")
      done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+' "${l_mod_chk_name//-/}_"' \b')
      if lsmod | grep "$l_mod_chk_name" &> /dev/null; then
        a_output2+=(" - unloading kernel module: \"$l_mod_name\"")
        modprobe -r "$l_mod_chk_name" 2>/dev/null; rmmod "$l_mod_name"
2>/dev/null
      fi
      if ! grep -Pq -- '\binstall\h+' "${l_mod_chk_name//-/}_"' \b' <<<
"${a_showconfig[*]}"; then
        a_output2+=(" - setting kernel module: \"$l_mod_name\" to
\"$(readlink -f /bin/false)\"")
        printf '%s\n' "install $l_mod_chk_name $(readlink -f /bin/false)" >>
/etc/modprobe.d/"$l_mod_name".conf
      fi
      if ! grep -Pq -- '\bblacklist\h+' "${l_mod_chk_name//-/}_"' \b' <<<
"${a_showconfig[*]}"; then
        a_output2+=(" - denylisting kernel module: \"$l_mod_name\"")
        printf '%s\n' "blacklist $l_mod_chk_name" >>
/etc/modprobe.d/"$l_mod_name".conf
      fi
    }
    for l_mod_base_directory in $l_mod_path; do # Check if the module exists
on the system
      if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
        a_output3+=(" - \"$l_mod_base_directory\"")
        l_mod_chk_name="$l_mod_name"
        [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="${l_mod_name::-2}"
        [ "$l_dl" != "y" ] && f_module_fix
      else
        printf '%s\n' " - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\""
      fi
    done
    [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
    [ "${#a_output2[@]}" -gt 0 ] && printf '%s\n' "" "${a_output2[@]}" ||
printf '%s\n' "" " - No changes needed"
    printf '%s\n' "" " - remediation of kernel module: \"$l_mod_name\"
complete" ""
  }
}
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1005, T1005.000            | TA0005  | M1050       |

### *1.1.1.9 Ensure usb-storage kernel module is not available (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 2 - Workstation
- STIG

#### **Description:**

USB storage provides a means to transfer and store files ensuring persistence and availability of the files independent of network connection status. Its popularity and utility has led to USB-based malware being a simple and common means for network infiltration and a first step to establishing a persistent threat within a networked environment.

#### **Rationale:**

Restricting USB access on the system will decrease the physical attack surface for a device and diminish the possible vectors to introduce malware.

#### **Impact:**

Disabling the **usb-storage** module will disable any usage of USB storage devices.

If requirements and local site policy allow the use of such devices, other solutions should be configured accordingly instead. One example of a commonly used solution is **USBGuard**.

#### **Audit:**

Run the following script to verify:

- **IF** - the **usb-storage** kernel module is available in ANY installed kernel, verify:

- An entry including **/bin/true** or **/bin/false** exists in a file within the **/etc/modprobe.d/** directory
- The module is deny listed in a file within the **/etc/modprobe.d/** directory
- The module is not loaded in the running kernel

- **IF** - the **usb-storage** kernel module is not available on the system, or pre-compiled into the kernel, no additional configuration is necessary

```

#!/usr/bin/env bash

{
    a_output=() a_output2=() a_output3=() l_dl="" l_mod_name="usb-storage"
    l_mod_type="drivers"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_chk()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if ! lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loaded")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loaded")
            fi
            if grep -Pq -- '\bbinstall\h+'${l_mod_chk_name//-/}_
/_}'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loadable")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loadable")
            fi
            if grep -Pq -- '\bbblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is deny listed")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is not deny listed")
            fi
        }
        for l_mod_base_directory in $l_mod_path; do
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name:-2)"
                [ "$l_dl" != "y" ] && f_module_chk
            else
                a_output+=(" - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\"")
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        if [ "${#a_output2[@]}" -le 0 ]; then
            printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}"
        else
            printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
            [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "- Correctly set:"
"${a_output[@]}"
        fi
    }
}

```

## Remediation:

Run the following script to unload and disable the `usb-storage` module:

- **IF** - the `usb-storage` kernel module is available in ANY installed kernel:

- Create a file ending in `.conf` with `install usb-storage /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist usb-storage` in the `/etc/modprobe.d/` directory
- Run `modprobe -r usb-storage 2>/dev/null; rmmod usb-storage 2>/dev/null` to remove `usb-storage` from the kernel

- **IF** - the `usb-storage` kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

```
#!/usr/bin/env bash

{
    a_output2=() a_output3=() l_dl="" l_mod_name="usb-storage"
l_mod_type="drivers"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_fix()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+' "${l_mod_chk_name//-/}_"' \b')
            if lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output2+=(" - unloading kernel module: \"$l_mod_name\"")
                modprobe -r "$l_mod_chk_name" 2>/dev/null; rmmod "$l_mod_name"
2>/dev/null
            fi
            if ! grep -Pq -- '\binstall\h+' "${l_mod_chk_name//-/}_"' \b' <<<
"${a_showconfig[*]}"; then
                a_output2+=(" - setting kernel module: \"$l_mod_name\" to
\"$(readlink -f /bin/false)\")
                printf '%s\n' "install $l_mod_chk_name $(readlink -f /bin/false)" >>
/etc/modprobe.d/"$l_mod_name".conf
            fi
            if ! grep -Pq -- '\bblacklist\h+' "${l_mod_chk_name//-/}_"' \b' <<<
"${a_showconfig[*]}"; then
                a_output2+=(" - denylisting kernel module: \"$l_mod_name\"")
                printf '%s\n' "blacklist $l_mod_chk_name" >>
/etc/modprobe.d/"$l_mod_name".conf
            fi
        }
        for l_mod_base_directory in $l_mod_path; do # Check if the module exists
on the system
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name::-2"
                [ "$l_dl" != "y" ] && f_module_fix
            else
                printf '%s\n' " - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\""
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        [ "${#a_output2[@]}" -gt 0 ] && printf '%s\n' "" "${a_output2[@]}" ||
printf '%s\n' "" " - No changes needed"
        printf '%s\n' "" " - remediation of kernel module: \"$l_mod_name\"
complete" ""
    }
}
```

## References:

1. NIST SP 800-53 Rev. 5: SI-3

## Additional Information:

An alternative solution to disabling the usb-storage module may be found in USBGuard.

Use of USBGuard and construction of USB device policies should be done in alignment with site policy.

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230503  
Rule ID: SV-230503r942936  
STIG ID: RHEL-08-040080  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                              | IG 1                                                                                | IG 2                                                                                 | IG 3                                                                                 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| v8               | <b>10.3 <u>Disable Autorun and Autoplay for Removable Media</u></b><br>Disable autorun and autoplay auto-execute functionality for removable media.                                                                                  |  |   |   |
| v7               | <b>13.7 <u>Manage USB Devices</u></b><br>If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained. |                                                                                     |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques                          | Tactics        | Mitigations |
|------------------------------------------------------|----------------|-------------|
| T1052, T1052.001, T1091, T1091.000, T1200, T1200.000 | TA0001, TA0010 | M1034       |



### *1.1.1.10 Ensure unused filesystems kernel modules are not available (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Filesystem kernel modules are pieces of code that can be dynamically loaded into the Linux kernel to extend its filesystem capabilities, or so-called base kernel, of an operating system. Filesystem kernel modules are typically used to add support for new hardware (as device drivers), or for adding system calls.

#### **Rationale:**

While loadable filesystem kernel modules are a convenient method of modifying the running kernel, this can be abused by attackers on a compromised system to prevent detection of their processes or files, allowing them to maintain control over the system. Many rootkits make use of loadable filesystem kernel modules in this way.

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it. The following filesystem kernel modules have known CVE's and should be made unavailable if no dependencies exist:

- **afs** - CVE-2022-37402
- **ceph** - CVE-2022-0670
- **cifs** - CVE-2022-29869
- **exfat** CVE-2022-29973
- **ext** CVE-2022-1184
- **fat** CVE-2022-22043
- **fscache** CVE-2022-3630
- **fuse** CVE-2023-0386
- **gfs2** CVE-2023-3212
- **nfs\_common** CVE-2023-6660
- **nfsd** CVE-2022-43945
- **smbfs\_common** CVE-2022-2585

#### **Impact:**

This list may be quite extensive and covering all edges cases is difficult. Therefore, it's crucial to carefully consider the implications and dependencies before making any changes to the filesystem kernel module configurations.

**Audit:**

Run the following script to:

- Look at the filesystem kernel modules available to the currently running kernel.
- Exclude mounted filesystem kernel modules that don't currently have a CVE
- List filesystem kernel modules that are not fully disabled, or are loaded into the kernel

Review the generated output

```

#!/usr/bin/env bash

{
  a_output=(); a_output2=(); a_modprobe_config=(); a_excluded=(); a_available_modules=()
  a_ignore=("xfs" "vfat" "ext2" "ext3" "ext4")
  a_cve_exists=("afs" "ceph" "cifs" "exfat" "ext" "fat" "fscache" "fuse" "gfs2" "nfs_common"
  "nfsd" "smbfs_common")
  f_module_chk()
  {
    l_out2=""; grep -Pq -- "\b$l_mod_name\b" <<< "${a_cve_exists[*]}" && l_out2=" <- CVE
exists!"
    if ! grep -Pq -- '\bblacklist\b' "$l_mod_name" <<< "${a_modprobe_config[*]"; then
      a_output2+=(" - Kernel module: \"$l_mod_name\" is not fully disabled $l_out2")
    elif ! grep -Pq -- '\binstall\b' "$l_mod_name" <<< "${a_modprobe_config[*]"; then
      a_output2+=(" - Kernel module: \"$l_mod_name\" is not fully disabled $l_out2")
    fi
    if lsmod | grep "$l_mod_name" &> /dev/null; then # Check if the module is currently loaded
      l_output2+=(" - Kernel module: \"$l_mod_name\" is loaded" "")
    fi
  }
  while IFS= read -r -d $'\0' l_module_dir; do
    a_available_modules+=("${basename "$l_module_dir"}")
    done < <(find "$(readlink -f /lib/modules/"$(uname -r)"/kernel/fs)" -mindepth 1 -maxdepth 1 -
type d ! -empty -print0)
    while IFS= read -r l_exclude; do
      if grep -Pq -- "\b$l_exclude\b" <<< "${a_cve_exists[*]"; then
        a_output2+=(" - ** WARNING: kernel module: \"$l_exclude\" has a CVE and is currently
mounted! **")
      elif
        grep -Pq -- "\b$l_exclude\b" <<< "${a_available_modules[*]"; then
          a_output+=(" - Kernel module: \"$l_exclude\" is currently mounted - do NOT unload or
disable")
        fi
        ! grep -Pq -- "\b$l_exclude\b" <<< "${a_ignore[*]"; && a_ignore+=("$l_exclude")
      done < <(findmnt -knD | awk '{print $2}' | sort -u)
      while IFS= read -r l_config; do
        a_modprobe_config+=("$l_config")
        done < <(modprobe --showconfig | grep -P '^h*(blacklist|install)')
        for l_mod_name in "${a_available_modules[@]"; do # Iterate over all filesystem modules
          [[ "$l_mod_name" =~ overlay ]] && l_mod_name="$l_mod_name:-2"
          if grep -Pq -- "\b$l_mod_name\b" <<< "${a_ignore[*]"; then
            a_excluded+=(" - Kernel module: \"$l_mod_name\"")
          else
            f_module_chk
          fi
        done
        [ "${#a_excluded[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" \
"The following intentionally skipped" \
"${a_excluded[@]}"
        if [ "${#a_output2[@]}" -le 0 ]; then
          printf '%s\n' "" " - No unused filesystem kernel modules are enabled" "${a_output[@]}" ""
        else
          printf '%s\n' "" " -- Audit Result: --" "" ** REVIEW the following **" "${a_output2[@]}"
          [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" " -- Correctly set: --" "${a_output[@]}" ""
        fi
      }
}

```

**WARNING:** disabling or denylisting filesystem modules that are in use on the system may be FATAL. It is extremely important to thoroughly review this list.

## Remediation:

- **IF** - the module is available in the running kernel:

- Unload the filesystem kernel module from the kernel
- Create a file ending in **.conf** with install filesystem kernel modules **/bin/false** in the **/etc/modprobe.d/** directory
- Create a file ending in **.conf** with deny list filesystem kernel modules in the **/etc/modprobe.d/** directory

**WARNING:** unloading, disabling or denylisting filesystem modules that are in use on the system maybe FATAL. It is extremely important to thoroughly review the filesystems returned by the audit before following the remediation procedure.

*Example of unloading the **gfs2** kernel module:*

```
# modprobe -r gfs2 2>/dev/null
# rmmod gfs2 2>/dev/null
```

*Example of fully disabling the **gfs2** kernel module:*

```
# printf '%s\n' "blacklist gfs2" "install gfs2 /bin/false" >>
/etc/modprobe.d/gfs2.conf
```

## Note:

- Disabling a kernel module by modifying the command above for each unused filesystem kernel module
- The example **gfs2** must be updated with the appropriate module name for the command or example script below to run correctly.

**Below is an example Script that can be modified to use on various filesystem kernel modules manual remediation process:**

*Example Script*

```

#!/usr/bin/env bash

{
    a_output2=(); a_output3=(); l_dl="" # Initialize arrays and clear
variables
    l_mod_name="gfs2" # set module name
    l_mod_type="fs" # set module type
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_fix()
    {
        l_dl="y" # Set to ignore duplicate checks
        a_showconfig=() # Create array with modprobe output
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_name//-/}_'\b')
            if lsmod | grep "$l_mod_name" &> /dev/null; then # Check if the module
is currently loaded
                a_output2+=(" - unloading kernel module: \"${l_mod_name}\"")
                modprobe -r "${l_mod_name}" 2>/dev/null; rmmod "${l_mod_name}"
2>/dev/null
            fi
            if ! grep -Pq -- '\binstall\h+'${l_mod_name//-/}_
/_'\b'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output2+=(" - setting kernel module: \"${l_mod_name}\" to
\"$(readlink -f /bin/false)\"")
                printf '%s\n' "install $l_mod_name $(readlink -f /bin/false)" >>
/etc/modprobe.d/"${l_mod_name}.conf
            fi
            if ! grep -Pq -- '\bblacklist\h+'${l_mod_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output2+=(" - denylisting kernel module: \"${l_mod_name}\"")
                printf '%s\n' "blacklist $l_mod_name" >>
/etc/modprobe.d/"${l_mod_name}.conf
            fi
        }
        for l_mod_base_directory in $l_mod_path; do # Check if the module exists
on the system
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}_/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}_/")" ]; then
                a_output3+=(" - \"${l_mod_base_directory}\"")
                [[ "$l_mod_name" =~ overlay ]] && l_mod_name="${l_mod_name::-2}"
                [ "$l_dl" != "y" ] && f_module_fix
            else
                echo -e " - kernel module: \"${l_mod_name}\" doesn't exist in
\"${l_mod_base_directory}\""
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"${l_mod_name}\" exists in:" "${a_output3[@]}"
        [ "${#a_output2[@]}" -gt 0 ] && printf '%s\n' "" "${a_output2[@]}" ||
printf '%s\n' "" " - No changes needed"
        printf '%s\n' "" " - remediation of kernel module: \"${l_mod_name}\"
complete" ""
    }
}

```

## References:

1. <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=filesystem>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

### *1.1.1.11 Ensure the operating system disables the ability to load the firewire-core kernel module (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must disable IEEE 1394 (FireWire) Support.

#### **Rationale:**

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

The IEEE 1394 (FireWire) is a serial bus standard for high-speed real-time communication. Disabling FireWire protects the system against exploitation of any flaws in its implementation.

#### **Audit:**

Verify the operating system disables the ability to load the firewire-core kernel module.

```
# grep -ri firewire-core /etc/modprobe.d/* | grep -i "/bin/false"

install firewire-core /bin/false
```

If the command does not return any output, or the line is commented out, and use of the firewire-core protocol is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Verify the operating system disables the ability to use the firewire-core kernel module. Check to see if the firewire-core kernel module is disabled with the following command:

```
# grep -ri firewire-core /etc/modprobe.d/* | grep -i "blacklist"

blacklist firewire-core
```

If the command does not return any output or the output is not "blacklist firewire-core", and use of the firewire-core kernel module is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

## Remediation:

Configure the operating system to disable the ability to use the firewire-core kernel module.

Add or update the following lines in the file `"/etc/modprobe.d/blacklist.conf"`:

```
install firewire-core /bin/false
blacklist firewire-core
```

Reboot the system for the settings to take effect.

## References:

1. NIST SP 800-53 Revision 5 :: CM-7 a
2. NIST SP 800-53A :: CM-7.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230499  
Rule ID: SV-230499r942933  
STIG ID: RHEL-08-040026  
Severity: CAT III

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      | ●    | ●    |
| v7               | <u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      | ●    | ●    |



### *1.1.1.12 Ensure a camera is not installed (Automated)*

**Profile Applicability:**

- STIG

**Description:**

The operating system must cover or disable the built-in or attached camera when not in use.

**Rationale:**

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Failing to disconnect from collaborative computing devices (i.e., cameras) can result in subsequent compromises of organizational information. Providing easy methods to physically disconnect from such devices after a collaborative computing session helps to ensure participants actually carry out the disconnect activity without having to go through complex and tedious procedures.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000370-GPOS-00155

## Audit:

If the device or operating system does not have a camera installed, this requirement is not applicable.

This requirement is not applicable to mobile devices (smartphones and tablets), where the use of the camera is a local AO decision.

This requirement is not applicable to dedicated VTC suites located in approved VTC locations that are centrally managed.

For an external camera, if there is not a method for the operator to manually disconnect the camera at the end of collaborative computing sessions, this is a finding.

For a built-in camera, the camera must be protected by a camera cover (e.g., laptop camera cover slide) when not in use. If the built-in camera is not protected with a camera cover, or is not physically disabled, this is a finding.

If the camera is not disconnected, covered, or physically disabled, determine if it is being disabled via software with the following commands:

Determine if the camera is disabled via blacklist with the following command:

```
# grep -r uvcvideo /etc/modprobe.d/* | grep "/bin/false"

install uvcvideo /bin/false
```

Determine if a camera is disabled via blacklist with the following command:

```
# grep -r uvcvideo /etc/modprobe.d/* | grep "blacklist"

blacklist uvcvideo
```

If the camera driver blacklist is missing, a camera driver is determined to be in use, and the collaborative computing device has not been authorized for use, this is a finding.

## Remediation:

Configure the operating system to disable the built-in or attached camera when not in use

Build or modify the "/etc/modprobe.d/blacklist.conf" file by using the following example:

```
##Disable WebCam
install uvcvideo /bin/false
blacklist uvcvideo
```

Reboot the system for the settings to take effect.

## References:

1. NIST SP 800-53 Revision 5 :: CM-7 a
2. NIST SP 800-53A :: CM-7.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230493  
Rule ID: SV-230493r942915  
STIG ID: RHEL-08-040020  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## 1.1.2 Configure Filesystem Partitions

Directories that are used for system-wide functions can be further protected by placing them on separate partitions. This provides protection for resource exhaustion and enables the use of mounting options that are applicable to the directory's intended use. Users' data can be stored on separate partitions and have stricter mount options. A user partition is a filesystem that has been established for use by the users and does not contain software for system operations.

The recommendations in this section are easier to perform during initial system installation. If the system is already installed, it is recommended that a full backup be performed before repartitioning the system.

### Note:

**-IF-** you are repartitioning a system that has already been installed (This may require the system to be in single-user mode):

- Mount the new partition to a temporary mountpoint e.g. `mount /dev/sda2 /mnt`
- Copy data from the original partition to the new partition. e.g. `cp -a /var/tmp/* /mnt`
- Verify that all data is present on the new partition. e.g. `ls -la /mnt`
- Unmount the new partition. e.g. `umount /mnt`
- Remove the data from the original directory that was in the old partition. e.g. `rm -Rf /var/tmp/*` Otherwise it will still consume space in the old partition that will be masked when the new filesystem is mounted.
- Mount the new partition to the desired mountpoint. e.g. `mount /dev/sda2 /var/tmp`
- Update `/etc/fstab` with the new mountpoint. e.g. `/dev/sda2 /var/tmp xfs defaults,rw,nosuid,nodev,noexec,relatime 0 0`

### 1.1.2.1 Configure /tmp

The `/tmp` directory is a world-writable directory used to store data used by the system and user applications for a short period of time. This data should have no expectation of surviving a reboot, as this directory is intended to be emptied after each reboot.

### 1.1.2.1.1 Ensure /tmp is a separate partition (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The `/tmp` directory is a world-writable directory used for temporary storage by all users and some applications.

- **IF** - an entry for `/tmp` exists in `/etc/fstab` it will take precedence over entries in systemd default unit file.

**Note:** In an environment where the main system is diskless and connected to iSCSI, entries in `/etc/fstab` may not take precedence.

`/tmp` can be configured to use `tmpfs`.

`tmpfs` puts everything into the kernel internal caches and grows and shrinks to accommodate the files it contains and is able to swap unneeded pages out to swap space. It has maximum size limits which can be adjusted on the fly via `mount -o remount`.

Since `tmpfs` lives completely in the page cache and on swap, all `tmpfs` pages will be shown as "Shmem" in `/proc/meminfo` and "Shared" in `free`. Notice that these counters also include shared memory. The most reliable way to get the count is using `df` and `du`.

`tmpfs` has three mount options for sizing:

- **size**: The limit of allocated bytes for this `tmpfs` instance. The default is half of your physical RAM without swap. If you oversize your `tmpfs` instances the machine will deadlock since the OOM handler will not be able to free that memory.
- **nr\_blocks**: The same as size, but in blocks of `PAGE_SIZE`.
- **nr\_inodes**: The maximum number of inodes for this instance. The default is half of the number of your physical RAM pages, or (on a machine with highmem) the number of lowmem RAM pages, whichever is the lower.

These parameters accept a suffix k, m or g and can be changed on remount. The size parameter also accepts a suffix % to limit this `tmpfs` instance to that percentage of your physical RAM. The default, when neither **size** nor **nr\_blocks** is specified, is **size=50%**.

**Rationale:**

Making `/tmp` its own file system allows an administrator to set additional mount options such as the `noexec` option on the mount, making `/tmp` useless for an attacker to install executable code. It would also prevent an attacker from establishing a hard link to a system `setuid` program and wait for it to be updated. Once the program was updated, the hard link would be broken, and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

This can be accomplished by either mounting `tmpfs` to `/tmp`, or creating a separate partition for `/tmp`.

**Impact:**

By design files saved to `/tmp` should have no expectation of surviving a reboot of the system. `tmpfs` is ram based, and all files stored to `tmpfs` will be lost when the system is rebooted.

If files need to be persistent through a reboot, they should be saved to `/var/tmp` not `/tmp`.

Since the `/tmp` directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to `tmpfs` or a separate partition.

Running out of `/tmp` space is a problem regardless of what kind of filesystem lies under it, but in a configuration where `/tmp` is not a separate file system it will essentially have the whole disk available, as the default installation only creates a single `/` partition. On the other hand, a RAM-based `/tmp` (as with `tmpfs`) will almost certainly be much smaller, which can lead to applications filling up the filesystem much more easily. Another alternative is to create a dedicated partition for `/tmp` from a separate volume or disk. One of the downsides of a disk-based dedicated partition is that it will be slower than `tmpfs` which is RAM-based.

## Audit:

Run the following command and verify the output shows that **/tmp** is mounted. Particular requirements pertaining to mount options are covered in ensuing sections.

```
# findmnt -kn /tmp
```

*Example output:*

```
/tmp tmpfs tmpfs rw,nosuid,nodev,noexec
```

Ensure that systemd will mount the **/tmp** partition at boot time.

```
# systemctl is-enabled tmp.mount
```

*Example output:*

```
generated
```

Verify output is not **masked** or **disabled**.

**Note:** By default, systemd will output **generated** if there is an entry in **/etc/fstab** for **/tmp**. This just means systemd will use the entry in **/etc/fstab** instead of its default unit file configuration for **/tmp**.

## Remediation:

First ensure that systemd is correctly configured to ensure that **/tmp** will be mounted at boot time.

```
# systemctl unmask tmp.mount
```

For specific configuration requirements of the **/tmp** mount for your environment, modify **/etc/fstab**.

Example of using **tmpfs** with specific mount options:

```
tmpfs /tmp tmpfs defaults,rw,nosuid,nodev,noexec,relatime,size=2G 0  
0
```

**Note:** the **size=2G** is an example of setting a specific size for **tmpfs**.

Example of using a volume or disk with specific mount options. The source location of the volume or disk will vary depending on your environment:

```
<device> /tmp <fstype> defaults,nodev,nosuid,noexec 0 0
```

## References:

1. <https://www.freedesktop.org/wiki/Software/systemd/APIFileSystems/>
2. <https://www.freedesktop.org/software/systemd/man/systemd-fstab-generator.html>
3. <https://www.kernel.org/doc/Documentation/filesystems/tmpfs.txt>
4. NIST SP 800-53 Rev. 5: CM-7



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230295  
Rule ID: SV-30295r627750  
STIG ID: RHEL-08-010543  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1499, T1499.001            | TA0005  | M1022       |

### 1.1.2.1.2 Ensure nodev option set on /tmp partition (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The **nodev** mount option specifies that the filesystem cannot contain special devices.

#### Rationale:

Since the **/tmp** filesystem is not intended to support devices, set this option to ensure that users cannot create a block or character special devices in **/tmp**.

#### Audit:

- **IF** - a separate partition exists for **/tmp**, verify that the **nodev** option is set.  
Run the following command to verify that the **nodev** mount option is set.

*Example:*

```
# findmnt -kn /tmp | grep -v nodev  
  
Nothing should be returned
```

#### Remediation:

- **IF** - a separate partition exists for **/tmp**.  
Edit the **/etc/fstab** file and add **nodev** to the fourth field (mounting options) for the **/tmp** partition.

*Example:*

```
<device> /tmp <fstype> defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

Run the following command to remount **/tmp** with the configured options:

```
# mount -o remount /tmp
```

#### References:

1. See the **fstab(5)** manual page for more information.
2. NIST SP 800-53 Rev. 5: CM-7
3. NIST SP 800-53 Revision 5 :: CM-7 (2)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230511  
Rule ID: SV-230511r854052  
STIG ID: RHEL-08-040123  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1200, T1200.000            | TA0005  | M1022       |

### 1.1.2.1.3 Ensure nosuid option set on /tmp partition (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The **nosuid** mount option specifies that the filesystem cannot contain **setuid** files.

#### Rationale:

Since the **/tmp** filesystem is only intended for temporary file storage, set this option to ensure that users cannot create **setuid** files in **/tmp**.

#### Audit:

- **IF** - a separate partition exists for **/tmp**, verify that the **nosuid** option is set. Run the following command to verify that the **nosuid** mount option is set.

*Example:*

```
# findmnt -kn /tmp | grep -v nosuid  
  
Nothing should be returned
```

#### Remediation:

- **IF** - a separate partition exists for **/tmp**.

Edit the **/etc/fstab** file and add **nosuid** to the fourth field (mounting options) for the **/tmp** partition.

*Example:*

```
<device> /tmp    <fstype>        defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

Run the following command to remount **/tmp** with the configured options:

```
# mount -o remount /tmp
```

#### References:

1. See the **fstab(5)** manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230512  
Rule ID: SV-230512r854053  
STIG ID: RHEL-08-040124  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1548, T1548.001            | TA0005  | M1022       |

#### 1.1.2.1.4 Ensure noexec option set on /tmp partition (Automated)

##### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

##### Description:

The **noexec** mount option specifies that the filesystem cannot contain executable binaries.

##### Rationale:

Since the **/tmp** filesystem is only intended for temporary file storage, set this option to ensure that users cannot run executable binaries from **/tmp**.

##### Impact:

Setting the **noexec** option on **/tmp** may prevent installation and/or updating of some 3rd party software.

##### Audit:

- **IF** - a separate partition exists for **/tmp**, verify that the **noexec** option is set. Run the following command to verify that the **noexec** mount option is set.

*Example:*

```
# findmnt -kn /tmp | grep -v noexec  
Nothing should be returned
```

##### Remediation:

- **IF** - a separate partition exists for **/tmp**. Edit the **/etc/fstab** file and add **noexec** to the fourth field (mounting options) for the **/tmp** partition.

*Example:*

```
<device> /tmp <fstype> defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

Run the following command to remount **/tmp** with the configured options:

```
# mount -o remount /tmp
```

## References:

1. See the `fstab(5)` manual page for more information.
2. NIST SP 800-53 Rev. 5: CM-7 (2)
3. CCI-001764

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230513  
Rule ID: SV-230513r854054  
STIG ID: RHEL-08-040125  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |    |    |    |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1204, T1204.002            | TA0005  | M1022       |

### 1.1.2.2 Configure /dev/shm

The `/dev/shm` directory is a world-writable directory that can function as shared memory that facilitates inter process communication (IPC)



### 1.1.2.2.1 Ensure /dev/shm is a separate partition (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The `/dev/shm` directory is a world-writable directory that can function as shared memory that facilitates inter process communication (IPC).

#### Rationale:

Making `/dev/shm` its own file system allows an administrator to set additional mount options such as the `noexec` option on the mount, making `/dev/shm` useless for an attacker to install executable code. It would also prevent an attacker from establishing a hard link to a system `setuid` program and wait for it to be updated. Once the program was updated, the hard link would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

This can be accomplished by mounting `tmpfs` to `/dev/shm`.

#### Impact:

Since the `/dev/shm` directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition.

`/dev/shm` utilizing `tmpfs` can be resized using the `size={size}` parameter in the relevant entry in `/etc/fstab`.

#### Audit:

- IF - `/dev/shm` is to be used on the system, run the following command and verify the output shows that `/dev/shm` is mounted. Particular requirements pertaining to mount options are covered in ensuing sections.

```
# findmnt -kn /dev/shm
```

*Example output:*

```
/dev/shm tmpfs tmpfs rw,nosuid,nodev,noexec,relatime,seclabel
```

## Remediation:

For specific configuration requirements of the `/dev/shm` mount for your environment, modify `/etc/fstab`.

*Example:*

```
tmpfs    /dev/shm          tmpfs
defaults,rw,nosuid,nodev,noexec,relatime,size=2G  0 0
```

## References:

1. <https://www.freedesktop.org/wiki/Software/systemd/APIFileSystems/>
2. <https://www.freedesktop.org/software/systemd/man/systemd-fstab-generator.html>
3. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      | ●    | ●    |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1499, T1499.001            | TA0005  | M1022       |

### 1.1.2.2.2 Ensure nodev option set on /dev/shm partition (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The **nodev** mount option specifies that the filesystem cannot contain special devices.

#### Rationale:

Since the **/dev/shm** filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create special devices in **/dev/shm** partitions.

#### Audit:

- **IF** - a separate partition exists for **/dev/shm**, verify that the **nodev** option is set.

```
# findmnt -kn /dev/shm | grep -v 'nodev'
```

Nothing should be returned

#### Remediation:

- **IF** - a separate partition exists for **/dev/shm**.

Edit the **/etc/fstab** file and add **nodev** to the fourth field (mounting options) for the **/dev/shm** partition. See the **fstab(5)** manual page for more information.

*Example:*

```
tmpfs /dev/shm tmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

Run the following command to remount **/dev/shm** with the configured options:

```
# mount -o remount /dev/shm
```

**Note:** It is recommended to use **tmpfs** as the device/filesystem type as **/dev/shm** is used as shared memory space by applications.

#### References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2
2. NIST SP 800-53 Revision 5 :: CM-7 (2)

## Additional Information:

Some distributions mount `/dev/shm` through other means and require `/dev/shm` to be added to `/etc/fstab` even though it is already being mounted on boot. Others may configure `/dev/shm` in other locations and may override `/etc/fstab` configuration. Consult the documentation appropriate for your distribution.

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230508  
Rule ID: SV-230508r854049  
STIG ID: RHEL-08-040120  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |    |    |    |
| v7               | <b>14.6 Protect Information through Access Control Lists</b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1200, T1200.000            | TA0005  | M1022       |

### 1.1.2.2.3 Ensure nosuid option set on /dev/shm partition (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The **nosuid** mount option specifies that the filesystem cannot contain **setuid** files.

#### Rationale:

Setting this option on a file system prevents users from introducing privileged programs onto the system and allowing non-root users to execute them.

#### Audit:

- **IF** - a separate partition exists for **/dev/shm**, verify that the **nosuid** option is set.

```
# findmnt -kn /dev/shm | grep -v 'nosuid'
```

Nothing should be returned

#### Remediation:

- **IF** - a separate partition exists for **/dev/shm**.

Edit the **/etc/fstab** file and add **nosuid** to the fourth field (mounting options) for the **/dev/shm** partition. See the **fstab(5)** manual page for more information.

*Example:*

```
tmpfs /dev/shm tmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

Run the following command to remount **/dev/shm** with the configured options:

```
# mount -o remount /dev/shm
```

**Note:** It is recommended to use **tmpfs** as the device/filesystem type as **/dev/shm** is used as shared memory space by applications.

#### References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2
2. NIST SP 800-53 Revision 5 :: CM-7 (2)

## Additional Information:

Some distributions mount `/dev/shm` through other means and require `/dev/shm` to be added to `/etc/fstab` even though it is already being mounted on boot. Others may configure `/dev/shm` in other locations and may override `/etc/fstab` configuration. Consult the documentation appropriate for your distribution.

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230509  
Rule ID: SV-230509r854050  
STIG ID: RHEL-08-040121  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |    |    |    |
| v7               | <b>14.6 Protect Information through Access Control Lists</b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1548, T1548.001            | TA0005  | M1038       |

#### 1.1.2.2.4 Ensure noexec option set on /dev/shm partition (Automated)

##### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

##### Description:

The **noexec** mount option specifies that the filesystem cannot contain executable binaries.

##### Rationale:

Setting this option on a file system prevents users from executing programs from shared memory. This deters users from introducing potentially malicious software on the system.

##### Audit:

- **IF** - a separate partition exists for **/dev/shm**, verify that the **noexec** option is set.

```
# findmnt -kn /dev/shm | grep -v 'noexec'
```

Nothing should be returned

##### Remediation:

- **IF** - a separate partition exists for **/dev/shm**.

Edit the **/etc/fstab** file and add **noexec** to the fourth field (mounting options) for the **/dev/shm** partition.

*Example:*

```
tmpfs /dev/shm tmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

Run the following command to remount **/dev/shm** with the configured options:

```
# mount -o remount /dev/shm
```

**Note:** It is recommended to use **tmpfs** as the device/filesystem type as **/dev/shm** is used as shared memory space by applications.

##### References:

1. See the **fstab(5)** manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2
3. NIST SP 800-53 Revision 5 :: CM-7 (2)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230510  
Rule ID: SV-230510r854051  
STIG ID: RHEL-08-040122  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1204, T1204.002            | TA0005  | M1022       |



### 1.1.2.3 Configure /home

Please note that home directories can be mounted anywhere and are not necessarily restricted to **/home**, nor restricted to a single location, nor is the name restricted in any way.

Finding user home directories can be done by looking in **/etc/passwd**, looking over the mounted file systems with **mount** or querying the relevant database with **getent**.

```
for user in $(awk -F ':' '{print $1}' /etc/passwd); do echo "${user} - $(sudo  
getent passwd ${user} | awk -F ':' '{print $NF}')
```

### *1.1.2.3.1 Ensure separate partition exists for /home (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

The `/home` directory is used to support disk storage needs of local users.

#### **Rationale:**

The default installation only creates a single `/` partition. Since the `/home` directory contains user generated data, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system as a whole. In addition, other operations on the system could fill up the disk unrelated to `/home` and impact all local users.

Configuring `/home` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nODEV`. These options limit an attacker's ability to create exploits on the system. In the case of `/home` options such as `usrquota/grpquota` may be considered to limit the impact that users can have on each other with regards to disk resource exhaustion. Other options allow for specific behavior. See `man mount` for exact details regarding filesystem-independent and filesystem-specific options.

As `/home` contains user data, care should be taken to ensure the security and integrity of the data and mount point.

#### **Impact:**

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

## Audit:

Run the following command and verify output shows **/home** is mounted:

```
# findmnt -kn /home  
  
/home    /dev/sdb  ext4    rw,nosuid,nodev,noexec,relatime,seclabel
```

## Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for **/home**.

For systems that were previously installed, create a new partition and configure **/etc/fstab** as appropriate.

## References:

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>
2. NIST SP 800-53 Rev. 5: CM-7

## Additional Information:

When modifying **/home** it is advisable to bring the system to emergency mode (so auditd is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multi-user mode.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1499, T1499.001                   | TA0005         | M1038              |

### 1.1.2.3.2 Ensure nodev option set on /home partition (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The **nodev** mount option specifies that the filesystem cannot contain special devices.

#### Rationale:

Since the **/home** filesystem is not intended to support devices, set this option to ensure that users cannot create a block or character special devices in **/home**.

#### Audit:

- **IF** - a separate partition exists for **/home**, verify that the **nodev** option is set.

Run the following command to verify that the **nodev** mount option is set.

*Example:*

```
# findmnt -kn /home | grep -v nodev
```

Nothing should be returned

#### Remediation:

- **IF** - a separate partition exists for **/home**.

Edit the **/etc/fstab** file and add **nodev** to the fourth field (mounting options) for the **/home** partition.

*Example:*

```
<device> /home    <fstype>          defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

Run the following command to remount **/home** with the configured options:

```
# mount -o remount /home
```

#### References:

1. See the **fstab(5)** manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1200, T1200.000            | TA0005  | M1038       |

### 1.1.2.3.3 Ensure nosuid option set on /home partition (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The **nosuid** mount option specifies that the filesystem cannot contain **setuid** files.

#### Rationale:

Since the **/home** filesystem is only intended for user file storage, set this option to ensure that users cannot create **setuid** files in **/home**.

#### Audit:

- **IF** - a separate partition exists for **/home**, verify that the **nosuid** option is set. Run the following command to verify that the **nosuid** mount option is set.

*Example:*

```
# findmnt -kn /home | grep -v nosuid  
  
Nothing should be returned
```

#### Remediation:

- **IF** - a separate partition exists for **/home**.

Edit the **/etc/fstab** file and add **nosuid** to the fourth field (mounting options) for the **/home** partition.

*Example:*

```
<device> /home    <fstype>          defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

Run the following command to remount **/home** with the configured options:

```
# mount -o remount /home
```

#### References:

1. See the **fstab(5)** manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1548, T1548.001            | TA0005  | M1022       |



### *1.1.2.3.4 Ensure a separate file system/partition has been created for non-privileged local interactive user home directories (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

A separate filesystem must be used for user home directories (such as /home or an equivalent).

#### **Rationale:**

The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.

#### **Audit:**

Verify that a separate file system/partition has been created for non-privileged local interactive user home directories.

Check the home directory assignment for all non-privileged users, users with a User Identifier (UID) greater than 1000, on the system with the following command:

```
# awk -F: '($3>=1000)&&($7 !~ /nologin/){print $1,$3,$6}' /etc/passwd  
adamsj 1001 /home/adamsj  
jacksonm 1002 /home/jacksonm  
smithj 1003 /home/smithj
```

The output of the command will give the directory/partition that contains the home directories for the non-privileged users on the system (in this example, "/home") and users' shell. All accounts with a valid shell (such as /bin/bash) are considered interactive users.

Check that a file system/partition has been created for the non-privileged interactive users with the following command:

Note: The partition of "/home" is used in the example.

```
# grep /home /etc/fstab  
UUID=333ada18 /home ext4 noatime,nobarrier,nodev 1 2
```

If a separate entry for the file system/partition containing the non-privileged interactive user home directories does not exist, this is a finding.

#### **Remediation:**

Migrate the "/home" directory onto a separate file system/partition.

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230328  
Rule ID: SV-230328r902723  
STIG ID: RHEL-08-010800  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### *1.1.2.3.5 Ensure file systems that contain user home directories are mounted with the nosuid option (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must prevent files with the setuid and setgid bit set from being executed on file systems that contain user home directories.

#### **Rationale:**

The "nosuid" mount option causes the system not to execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setgid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

#### **Audit:**

Verify file systems that contain user home directories are mounted with the "nosuid" option.

Note: If a separate file system has not been created for the user home directories (user home directories are mounted under "/"), this is automatically a finding as the "nosuid" option cannot be used on the "/" system.

Find the file system(s) that contain the user home directories with the following command:

```
# awk -F: '($3>=1000)&&($7 !~ /nologin/){print $1,$3,$6}' /etc/passwd  
  
smithj:1001: /home/smithj  
robinst:1002: /home/robinst
```

Check the file systems that are mounted at boot time with the following command:

```
# more /etc/fstab  
  
UUID=a411dc99-f2a1-4c87-9e05-184977be8539 /home xfs  
rw,relatime,discard,data=ordered,nosuid,nodev,noexec 0 0
```

If a file system found in "/etc/fstab" refers to the user home directory file system and it does not have the "nosuid" option set, this is a finding.

#### **Remediation:**

Configure "/etc/fstab" to use the "nosuid" option on file systems that contain user home directories for interactive users.

## References:

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230299  
Rule ID: SV-230299r627750  
STIG ID: RHEL-08-010570  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |    |    |    |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### 1.1.2.3.6 Ensure file systems that contain user home directories are mounted with the "noexec" option (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must prevent code from being executed on file systems that contain user home directories.

#### Rationale:

The "noexec" mount option causes the system not to execute binary files. This option must be used for mounting any file system not containing approved binary files, as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

#### Audit:

Verify file systems that contain user home directories are mounted with the "noexec" option.

Note: If a separate file system has not been created for the user home directories (user home directories are mounted under "/"), this is automatically a finding as the "noexec" option cannot be used on the "/" system.

Find the file system(s) that contain the user home directories with the following command:

```
# awk -F: '($3>=1000)&&($7 !~ /nologin/){print $1,$3,$6}' /etc/passwd  
smithj:1001: /home/smithj  
robininst:1002: /home/robininst
```

Check the file systems that are mounted at boot time with the following command:

```
# more /etc/fstab  
UUID=a411dc99-f2a1-4c87-9e05-184977be8539 /home ext4  
rw,relatime,discard,data=ordered,nosuid,nodev,noexec 0 2
```

If a file system found in "/etc/fstab" refers to the user home directory file system and it does not have the "noexec" option set, this is a finding.

#### Remediation:

Configure the "/etc/fstab" to use the "noexec" option on file systems that contain user home directories for interactive users.

## References:

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230302  
Rule ID: SV-230302r627750  
STIG ID: RHEL-08-010590  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |    |    |    |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### 1.1.2.4 Configure /var

The `/var` directory is used by daemons and other system services to temporarily store dynamic data. Some directories created by these processes may be world-writable.

### *1.1.2.4.1 Ensure separate partition exists for /var (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### **Description:**

The `/var` directory is used by daemons and other system services to temporarily store dynamic data. Some directories created by these processes may be world-writable.

#### **Rationale:**

The reasoning for mounting `/var` on a separate partition is as follows.

The default installation only creates a single `/` partition. Since the `/var` directory may contain world writable files and directories, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system. In addition, other operations on the system could fill up the disk unrelated to `/var` and cause unintended behavior across the system as the disk is full. See `man auditd.conf` for details.

Configuring `/var` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nodev`. These options limit an attacker's ability to create exploits on the system. Other options allow for specific behavior. See `man mount` for exact details regarding filesystem-independent and filesystem-specific options.

An example of exploiting `/var` may be an attacker establishing a hard-link to a system `setuid` program and waiting for it to be updated. Once the program is updated, the hard-link can be broken and the attacker would have their own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

#### **Impact:**

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.



## Audit:

Run the following command and verify output shows **/var** is mounted.

*Example:*

```
# findmnt -kn /var  
  
/var /dev/sdb ext4 rw,nosuid,nodev,noexec,relatime,seclabel
```

## Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for **/var**.

For systems that were previously installed, create a new partition and configure **/etc/fstab** as appropriate.

## References:

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

When modifying **/var** it is advisable to bring the system to emergency mode (so auditd is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multi-user mode.

```
Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024  
  
GROUP ID: V-230292  
RULE ID: SV-230292r902718  
STIG ID: RHEL-08-010540  
SEVERITY: CAT III
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 Protect Information through Access Control Lists</b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1499, T1499.001                   | TA0006         | M1022              |

### 1.1.2.4.2 Ensure nodev option set on /var partition (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The **nodev** mount option specifies that the filesystem cannot contain special devices.

#### Rationale:

Since the **/var** filesystem is not intended to support devices, set this option to ensure that users cannot create a block or character special devices in **/var**.

#### Audit:

- **IF** - a separate partition exists for **/var**, verify that the **nodev** option is set.  
Run the following command to verify that the **nodev** mount option is set.

*Example:*

```
# findmnt -kn /var | grep -v nodev  
  
Nothing should be returned
```

#### Remediation:

- **IF** - a separate partition exists for **/var**.  
Edit the **/etc/fstab** file and add **nodev** to the fourth field (mounting options) for the **/var** partition.

*Example:*

```
<device> /var    <fstype>        defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

Run the following command to remount **/var** with the configured options:

```
# mount -o remount /var
```

#### References:

1. See the `fstab(5)` manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1200, T1200.000            | TA0005  | M1022       |

### 1.1.2.4.3 Ensure nosuid option set on /var partition (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The **nosuid** mount option specifies that the filesystem cannot contain **setuid** files.

#### Rationale:

Since the **/var** filesystem is only intended for variable files such as logs, set this option to ensure that users cannot create **setuid** files in **/var**.

#### Audit:

- **IF** - a separate partition exists for **/var**, verify that the **nosuid** option is set.

Run the following command to verify that the **nosuid** mount option is set.

*Example:*

```
# findmnt -kn /var | grep -v nosuid
```

Nothing should be returned

#### Remediation:

- **IF** - a separate partition exists for **/var**.

Edit the **/etc/fstab** file and add **nosuid** to the fourth field (mounting options) for the **/var** partition.

*Example:*

```
<device> /var <fstype> defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

Run the following command to remount **/var** with the configured options:

```
# mount -o remount /var
```

#### References:

1. See the **fstab(5)** manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1548, T1548.001            | TA0005  | M1022       |

### 1.1.2.5 Configure /var/tmp

The `/var/tmp` directory is a world-writable directory used for temporary storage by all users and some applications. Temporary files residing in `/var/tmp` are to be preserved between reboots.

### 1.1.2.5.1 Ensure separate partition exists for /var/tmp (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### Description:

The `/var/tmp` directory is a world-writable directory used for temporary storage by all users and some applications. Temporary files residing in `/var/tmp` are to be preserved between reboots.

#### Rationale:

The default installation only creates a single `/` partition. Since the `/var/tmp` directory is world-writable, there is a risk of resource exhaustion. In addition, other operations on the system could fill up the disk unrelated to `/var/tmp` and cause potential disruption to daemons as the disk is full.

Configuring `/var/tmp` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nodev`. These options limit an attacker's ability to create exploits on the system.

#### Impact:

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

#### Audit:

Run the following command and verify output shows `/var/tmp` is mounted.

*Example:*

```
# findmnt -kn /var/tmp  
  
/var/tmp    /dev/sdb ext4    rw,nosuid,nodev,noexec,relatime,seclabel
```

#### Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/var/tmp`.

For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.



## References:

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>
2. NIST SP 800-53 Rev. 5: CM-7
3. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

When modifying `/var/tmp` it is advisable to bring the system to emergency mode (so auditd is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multi-user mode.

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-244529  
Rule ID: SV-244529r902737  
STIG ID: RHEL-08-010544  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1499, T1499.001            | TA0005  | M1022       |

### 1.1.2.5.2 Ensure nodev option set on /var/tmp partition (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The **nodev** mount option specifies that the filesystem cannot contain special devices.

#### Rationale:

Since the **/var/tmp** filesystem is not intended to support devices, set this option to ensure that users cannot create a block or character special devices in **/var/tmp**.

#### Audit:

- **IF** - a separate partition exists for **/var/tmp**, verify that the **nodev** option is set. Run the following command to verify that the **nodev** mount option is set.

*Example:*

```
# findmnt -kn /var/tmp | grep -v nodev  
  
Nothing should be returned
```

#### Remediation:

- **IF** - a separate partition exists for **/var/tmp**. Edit the **/etc/fstab** file and add **nodev** to the fourth field (mounting options) for the **/var/tmp** partition.

*Example:*

```
<device> /var/tmp    <fstype>           defaults,rw,nosuid,nodev,noexec,relatime 0  
0
```

Run the following command to remount **/var/tmp** with the configured options:

```
# mount -o remount /var/tmp
```

#### References:

1. See the **fstab(5)** manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2
3. NIST SP 800-53 Revision 5 :: CM-7 (2)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230520  
Rule ID: SV-230520r854061  
STIG ID: RHEL-08-040132  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1499, T1499.001            | TA0005  | M1022       |

### 1.1.2.5.3 Ensure nosuid option set on /var/tmp partition (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The **nosuid** mount option specifies that the filesystem cannot contain **setuid** files.

#### Rationale:

Since the **/var/tmp** filesystem is only intended for temporary file storage, set this option to ensure that users cannot create **setuid** files in **/var/tmp**.

#### Audit:

- **IF** - a separate partition exists for **/var/tmp**, verify that the **nosuid** option is set. Run the following command to verify that the **nosuid** mount option is set.

*Example:*

```
# findmnt -kn /var/tmp | grep -v nosuid  
  
Nothing should be returned
```

#### Remediation:

- **IF** - a separate partition exists for **/var/tmp**. Edit the **/etc/fstab** file and add **nosuid** to the fourth field (mounting options) for the **/var/tmp** partition.

*Example:*

```
<device> /var/tmp    <fstype>          defaults,rw,nosuid,nodev,noexec,relatime 0  
0
```

Run the following command to remount **/var/tmp** with the configured options:

```
# mount -o remount /var/tmp
```

#### References:

1. See the **fstab(5)** manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2
3. NIST SP 800-53 Revision 5 :: CM-7 (2)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230521  
Rule ID: SV-230521r854062  
STIG ID: RHEL-08-040133  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1548, T1548.001            | TA0005  | M1022       |

### 1.1.2.5.4 Ensure noexec option set on /var/tmp partition (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The **noexec** mount option specifies that the filesystem cannot contain executable binaries.

#### Rationale:

Since the **/var/tmp** filesystem is only intended for temporary file storage, set this option to ensure that users cannot run executable binaries from **/var/tmp**.

#### Audit:

- **IF** - a separate partition exists for **/var/tmp**, verify that the **noexec** option is set. Run the following command to verify that the **noexec** mount option is set.

*Example:*

```
# findmnt -kn /var/tmp | grep -v noexec  
  
Nothing should be returned
```

#### Remediation:

- **IF** - a separate partition exists for **/var/tmp**.

Edit the **/etc/fstab** file and add **noexec** to the fourth field (mounting options) for the **/var/tmp** partition.

*Example:*

```
<device> /var/tmp    <fstype>           defaults,rw,nosuid,nodev,noexec,relatime 0  
0
```

Run the following command to remount **/var/tmp** with the configured options:

```
# mount -o remount /var/tmp
```

#### References:

1. See the **fstab(5)** manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2
3. NIST SP 800-53 Revision 5 :: CM-7 (2)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230522  
Rule ID: SV-230522r854063  
STIG ID: RHEL-08-040134  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1204, T1204.002            | TA0005  | M1022       |

### 1.1.2.6 Configure `/var/log`

The `/var/log` directory is used by system services to store log data.



### 1.1.2.6.1 Ensure separate partition exists for /var/log (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### Description:

The `/var/log` directory is used by system services to store log data.

#### Rationale:

The default installation only creates a single `/` partition. Since the `/var/log` directory contains log files which can grow quite large, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system as a whole.

Configuring `/var/log` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nodev`. These options limit an attacker's ability to create exploits on the system. Other options allow for specific behavior. See `man mount` for exact details regarding filesystem-independent and filesystem-specific options.

As `/var/log` contains log files, care should be taken to ensure the security and integrity of the data and mount point.

#### Impact:

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

#### Audit:

Run the following command and verify output shows `/var/log` is mounted:

```
# findmnt -kn /var/log  
  
/var/log /dev/sdb ext4    rw,nosuid,nodev,noexec,relatime,seclabel
```

#### Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/var/log`.

For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

## References:

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>
2. NIST SP 800-53 Rev. 5:: CM-6 b CM-7
3. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

When modifying **/var/log** it is advisable to bring the system to emergency mode (so auditd is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multiuser mode.

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230293  
Rule ID: SV-230293r902720  
STIG ID: RHEL-08-010541  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                         | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.3 <u>Ensure Adequate Audit Log Storage</u></b><br>Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process. |  |  |  |
| v7               | <b>6.4 <u>Ensure adequate storage for logs</u></b><br>Ensure that all systems that store logs have adequate storage space for the logs generated.                               |                                                                                       |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1499, T1499.001            | TA0005  | M1022       |

### 1.1.2.6.2 Ensure nodev option set on /var/log partition (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The **nodev** mount option specifies that the filesystem cannot contain special devices.

#### Rationale:

Since the **/var/log** filesystem is not intended to support devices, set this option to ensure that users cannot create a block or character special devices in **/var/log**.

#### Audit:

- **IF** - a separate partition exists for **/var/log**, verify that the **nodev** option is set. Run the following command to verify that the **nodev** mount option is set.

*Example:*

```
# findmnt -kn /var/log | grep -v nodev  
  
Nothing should be returned
```

#### Remediation:

- **IF** - a separate partition exists for **/var/log**. Edit the **/etc/fstab** file and add **nodev** to the fourth field (mounting options) for the **/var/log** partition.

*Example:*

```
<device> /var/log    <fstype>           defaults,rw,nosuid,nodev,noexec,relatime 0  
0
```

Run the following command to remount **/var/log** with the configured options:

```
# mount -o remount /var/log
```

#### References:

1. See the **fstab(5)** manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2
3. NIST SP 800-53 Revision 5 :: CM-7 (2)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230514  
Rule ID: SV-230514r854055  
STIG ID: RHEL-08-040126  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1200, T1200.000            | TA0005  | M1038       |

### 1.1.2.6.3 Ensure nosuid option set on /var/log partition (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The **nosuid** mount option specifies that the filesystem cannot contain **setuid** files.

#### Rationale:

Since the **/var/log** filesystem is only intended for log files, set this option to ensure that users cannot create **setuid** files in **/var/log**.

#### Audit:

- **IF** - a separate partition exists for **/var/log**, verify that the **nosuid** option is set. Run the following command to verify that the **nosuid** mount option is set.

*Example:*

```
# findmnt -kn /var/log | grep -v nosuid  
  
Nothing should be returned
```

#### Remediation:

- **IF** - a separate partition exists for **/var/log**. Edit the **/etc/fstab** file and add **nosuid** to the fourth field (mounting options) for the **/var/log** partition.

*Example:*

```
<device> /var/log    <fstype>           defaults,rw,nosuid,nodev,noexec,relatime 0  
0
```

Run the following command to remount **/var/log** with the configured options:

```
# mount -o remount /var/log
```

#### References:

1. See the **fstab(5)** manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2
3. NIST SP 800-53 Revision 5 :: CM-7 (2)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230515  
Rule ID: SV-230515r854056  
STIG ID: RHEL-08-040127  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1548, T1548.001            | TA0005  | M1022       |

### 1.1.2.6.4 Ensure noexec option set on /var/log partition (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The **noexec** mount option specifies that the filesystem cannot contain executable binaries.

#### Rationale:

Since the **/var/log** filesystem is only intended for log files, set this option to ensure that users cannot run executable binaries from **/var/log**.

#### Audit:

- **IF** - a separate partition exists for **/var/log**, verify that the **noexec** option is set. Run the following command to verify that the **noexec** mount option is set.

*Example:*

```
# findmnt -kn /var/log | grep -v noexec  
  
Nothing should be returned
```

#### Remediation:

- **IF** - a separate partition exists for **/var/log**.

Edit the **/etc/fstab** file and add **noexec** to the fourth field (mounting options) for the **/var/log** partition.

*Example:*

```
<device> /var/log    <fstype>           defaults,rw,nosuid,nodev,noexec,relatime 0  
0
```

Run the following command to remount **/var/log** with the configured options:

```
# mount -o remount /var/log
```

#### References:

1. See the **fstab(5)** manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2
3. NIST SP 800-53 Revision 5 :: CM-7 (2)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230516  
Rule ID: SV-230516r854057  
STIG ID: RHEL-08-040128  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1204, T1204.002            | TA0005  | M1022       |



### 1.1.2.7 Configure `/var/log/audit`

The auditing daemon, `auditd`, stores log data in the `/var/log/audit` directory.

### *1.1.2.7.1 Ensure separate partition exists for /var/log/audit (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### **Description:**

The auditing daemon, `auditd`, stores log data in the `/var/log/audit` directory.

#### **Rationale:**

The default installation only creates a single `/` partition. Since the `/var/log/audit` directory contains the `audit.log` file which can grow quite large, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system as a whole. In addition, other operations on the system could fill up the disk unrelated to `/var/log/audit` and cause `auditd` to trigger its `space_left_action` as the disk is full. See `man auditd.conf` for details.

Configuring `/var/log/audit` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nODEV`. These options limit an attacker's ability to create exploits on the system. Other options allow for specific behavior. See `man mount` for exact details regarding filesystem-independent and filesystem-specific options.

As `/var/log/audit` contains audit logs, care should be taken to ensure the security and integrity of the data and mount point.

#### **Impact:**

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

## Audit:

Run the following command and verify output shows `/var/log/audit` is mounted:

```
# findmnt -kn /var/log/audit  
  
/var/log/audit /dev/sdb ext4    rw,nosuid,nodev,noexec,relatime,seclabel
```

## Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/var/log/audit`.

For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

## References:

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>
2. NIST SP 800-53 Rev. 5: CM-7 CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

When modifying `/var/log/audit` it is advisable to bring the system to emergency mode (so auditd is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multi-user mode.

```
Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024  
  
Vul ID: V-230294  
Rule ID: SV-230294r627750  
STIG ID: RHEL-08-010542  
Severity: CAT II
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                  | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.3 Ensure Adequate Audit Log Storage</b><br>Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process. |  |  |  |
| v7               | <b>6.4 Ensure adequate storage for logs</b><br>Ensure that all systems that store logs have adequate storage space for the logs generated.                               |                                                                                       |  |  |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1499, T1499.001                   | TA0005         | M1022              |

### 1.1.2.7.2 Ensure nodev option set on /var/log/audit partition (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The **nodev** mount option specifies that the filesystem cannot contain special devices.

#### Rationale:

Since the **/var/log/audit** filesystem is not intended to support devices, set this option to ensure that users cannot create a block or character special devices in **/var/log/audit**.

#### Audit:

- **IF** - a separate partition exists for **/var/log/audit**, verify that the **nodev** option is set. Run the following command to verify that the **nodev** mount option is set.

*Example:*

```
# findmnt -kn /var/log/audit | grep -v nodev  
  
Nothing should be returned
```

#### Remediation:

- **IF** - a separate partition exists for **/var/log/audit**.

Edit the **/etc/fstab** file and add **nodev** to the fourth field (mounting options) for the **/var/log/audit** partition.

*Example:*

```
<device> /var/log/audit <fstype>  
defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

Run the following command to remount **/var/log/audit** with the configured options:

```
# mount -o remount /var/log/audit
```

#### References:

1. See the **fstab(5)** manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2
3. NIST SP 800-53 Revision 5 :: CM-7 (2)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230517  
Rule ID: SV-230517r854058  
STIG ID: RHEL-08-040129  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1200, T1200.000            | TA0005  | M1022       |

### 1.1.2.7.3 Ensure nosuid option set on /var/log/audit partition (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The **nosuid** mount option specifies that the filesystem cannot contain **setuid** files.

#### Rationale:

Since the **/var/log/audit** filesystem is only intended for variable files such as logs, set this option to ensure that users cannot create **setuid** files in **/var/log/audit**.

#### Audit:

- **IF** - a separate partition exists for **/var/log/audit**, verify that the **nosuid** option is set.

Run the following command to verify that the **nosuid** mount option is set.

*Example:*

```
# findmnt -kn /var/log/audit | grep -v nosuid  
  
Nothing should be returned
```

#### Remediation:

- **IF** - a separate partition exists for **/var/log/audit**.

Edit the **/etc/fstab** file and add **nosuid** to the fourth field (mounting options) for the **/var/log/audit** partition.

*Example:*

```
<device> /var/log/audit <fstype>  
defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

Run the following command to remount **/var/log/audit** with the configured options:

```
# mount -o remount /var/log/audit
```

#### References:

1. See the **fstab(5)** manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2
3. NIST SP 800-53 Revision 5 :: CM-7 (2)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230518  
Rule ID: SV-230518r854059  
STIG ID: RHEL-08-040130  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1548, T1548.001            | TA0005  | M1022       |



#### 1.1.2.7.4 Ensure noexec option set on /var/log/audit partition (Automated)

##### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

##### Description:

The **noexec** mount option specifies that the filesystem cannot contain executable binaries.

##### Rationale:

Since the **/var/log/audit** filesystem is only intended for audit logs, set this option to ensure that users cannot run executable binaries from **/var/log/audit**.

##### Audit:

- **IF** - a separate partition exists for **/var/log/audit**, verify that the **noexec** option is set.

Run the following command to verify that the **noexec** mount option is set.

*Example:*

```
# findmnt -kn /var/log/audit | grep -v noexec  
  
Nothing should be returned
```

##### Remediation:

- **IF** - a separate partition exists for **/var/log/audit**.

Edit the **/etc/fstab** file and add **noexec** to the fourth field (mounting options) for the **/var/log/audit** partition.

*Example:*

```
<device> /var/log/audit    <fstype>  
defaults,rw,nosuid,nodev,noexec,relatime 0 0
```

Run the following command to remount **/var/log/audit** with the configured options:

```
# mount -o remount /var/log/audit
```

##### References:

1. See the **fstab(5)** manual page for more information.
2. NIST SP 800-53 Rev. 5: AC-3, MP-2
3. NIST SP 800-53 Revision 5 :: CM-7 (2)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230519  
Rule ID: SV-230519r854060  
STIG ID: RHEL-08-040131  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1204, T1204.002            | TA0005  | M1022       |

### **1.1.2.8 Configure /boot**

### *1.1.2.8.1 Ensure the "/boot" directory is mounted with the "nosuid" option (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must prevent files with the "setuid" and "setgid" bit set from being executed on the "/boot" directory.

#### **Rationale:**

The "nosuid" mount option causes the system not to execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setgid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

#### **Audit:**

For systems that use UEFI, this is Not Applicable.

Verify the /boot directory is mounted with the "nosuid" option with the following command:

```
# mount | grep '\s/boot\s'

/dev/sda1 on /boot type xfs
(rw,nosuid,relatime,seclabe,attr2,inode64,noquota)
```

If the "/boot" file system does not have the "nosuid" option set, this is a finding.

#### **Remediation:**

Configure the "/etc/fstab" to use the "nosuid" option on the /boot directory.

#### **References:**

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230300  
Rule ID: SV-230300r743959  
STIG ID: RHEL-08-010571  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### 1.1.2.9 Configure /boot/efi

### *1.1.2.9.1 Ensure the "/boot/efi" directory is mounted with the "nosuid" option (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must prevent files with the "setuid" and "setgid" bit set from being executed on the "/boot/efi" directory.

#### **Rationale:**

The "nosuid" mount option causes the system not to execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setgid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

#### **Audit:**

For systems that use BIOS, this is Not Applicable.

Verify the "/boot/efi" directory is mounted with the "nosuid" option with the following command:

```
# mount | grep '\s/boot/efi\s'

/dev/sda1 on /boot/efi type xfs
(rw,nosuid,relatime,seclabe,attr2,inode64,noquota)
```

If the "/boot/efi" file system does not have the "nosuid" option set, this is a finding.

#### **Remediation:**

Configure the "/etc/fstab" to use the "nosuid" option on the "/boot/efi" directory.

#### **References:**

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244530  
Rule ID: SV-244530r809336  
STIG ID: RHEL-08-010572  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |



### **1.1.2.10 Configure nfs filesystems**

### *1.1.2.10.1 Ensure file systems that are being NFS-imported are mounted with the "nodev" option (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must prevent special devices on file systems that are imported via Network File System (NFS).

#### **Rationale:**

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

#### **Audit:**

Verify file systems that are being NFS-imported are mounted with the "nodev" option with the following command:

```
# grep nfs /etc/fstab | grep nodev  
  
UUID=e06097bb-cfcd-437b-9e4d-a691f5662a7d /store nfs rw,nosuid,nodev,noexec 0  
0
```

If a file system found in "/etc/fstab" refers to NFS and it does not have the "nodev" option set, this is a finding.

#### **Remediation:**

Configure the "/etc/fstab" to use the "nodev" option on file systems that are being imported via NFS.

#### **References:**

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230307  
Rule ID: SV-230307r627750  
STIG ID: RHEL-08-010640  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### *1.1.2.10.2 Ensure file systems being imported via NFS are mounted with the "nosuid" option (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must prevent files with the setuid and setgid bit set from being executed on file systems that are imported via Network File System (NFS).

#### **Rationale:**

The "nosuid" mount option causes the system not to execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setgid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

#### **Audit:**

Verify that file systems being imported via NFS are mounted with the "nosuid" option with the following command:

```
# grep nfs /etc/fstab | grep nosuid  
UUID=e06097bb-cfcd-437b-9e4d-a691f5662a7d /store nfs rw,nosuid,nodev,noexec 0  
0
```

If a file system found in "/etc/fstab" refers to NFS and it does not have the "nosuid" option set, this is a finding.

#### **Remediation:**

Configure the "/etc/fstab" to use the "nosuid" option on file systems that are being imported via NFS.

#### **References:**

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230308  
Rule ID: SV-230308r627750  
STIG ID: RHEL-08-010650  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### *1.1.2.10.3 Ensure file systems being imported via NFS are mounted with the "noexec" option (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must prevent code from being executed on file systems that are imported via Network File System (NFS).

#### **Rationale:**

The "noexec" mount option causes the system not to execute binary files. This option must be used for mounting any file system not containing approved binary as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

#### **Audit:**

Verify that file systems being imported via NFS are mounted with the "noexec" option with the following command:

```
# grep nfs /etc/fstab | grep noexec  
UUID=e06097bb-cfcd-437b-9e4d-a691f5662a7d /store nfs rw,nosuid,nodev,noexec 0  
0
```

If a file system found in "/etc/fstab" refers to NFS and it does not have the "noexec" option set, this is a finding.

#### **Remediation:**

Configure the "/etc/fstab" to use the "noexec" option on file systems that are being imported via NFS.

#### **References:**

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230306  
Rule ID: SV-230306r627750  
STIG ID: RHEL-08-010630  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### **1.1.2.11 Configure removable media partitions**



### 1.1.2.11.1 Ensure nodev option set on removable media partitions (Manual)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The **nodev** mount option specifies that the filesystem cannot contain special devices.

#### Rationale:

Removable media containing character and block special devices could be used to circumvent security controls by allowing non-root users to access sensitive device files such as **/dev/kmem** or the raw disk partitions.

#### Audit:

Run the following command and verify that the **nodev** option is set on all removable media partitions.

```
# more /etc/fstab
UUID=2bc871e4-e2a3-4f29-9ece-3be60c835222 /mnt/usbflash vfat
noauto,owner,ro,nosuid,nodev,noexec 0 0
```

If a file system found in **/etc/fstab** refers to removable media and it does not have the **"nodev"** option set, this is a finding.

#### Remediation:

Edit the **/etc/fstab** file and add **nodev** to the fourth field (mounting options) of all removable media partitions. Look for entries that have mount points that contain words such as floppy or cdrom. See the **fstab(5)** manual page for more information.

#### References:

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230303  
Rule ID: SV-230303r627750  
STIG ID: RHEL-08-010600  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### 1.1.2.11.2 Ensure nosuid option set on removable media partitions (Manual)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The **nosuid** mount option specifies that the filesystem cannot contain **setuid** files.

#### Rationale:

Setting this option on a file system prevents users from introducing privileged programs onto the system and allowing non-root users to execute them.

#### Audit:

Run the following command and verify that the **nosuid** option is set on all removable media partitions.

```
# more /etc/fstab  
  
UUID=2bc871e4-e2a3-4f29-9ece-3be60c835222 /mnt/usbflash vfat  
noauto,owner,ro,nosuid,nodev,noexec 0 0
```

If a file system found in "/etc/fstab" refers to removable media and it does not have the "nosuid" option set, this is a finding.

#### Remediation:

Edit the **/etc/fstab** file and add **nosuid** to the fourth field (mounting options) of all removable media partitions. Look for entries that have mount points that contain words such as floppy or cdrom. See the **fstab(5)** manual page for more information.

#### References:

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230305  
Rule ID: SV-230305r627750  
STIG ID: RHEL-08-010620  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### 1.1.2.11.3 Ensure noexec option set on removable media partitions (Manual)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The **noexec** mount option specifies that the filesystem cannot contain executable binaries.

#### Rationale:

Setting this option on a file system prevents users from executing programs from the removable media. This deters users from being able to introduce potentially malicious software on the system.

#### Audit:

Run the following command and verify that the **noexec** option is set on all removable media partitions.

```
# more /etc/fstab
UUID=2bc871e4-e2a3-4f29-9ece-3be60c835222 /mnt/usbflash vfat
noauto,owner,ro,nosuid,nodev,noexec 0 0
```

If a file system found in "/etc/fstab" refers to removable media and it does not have the "noexec" option set, this is a finding.

#### Remediation:

Edit the **/etc/fstab** file and add **noexec** to the fourth field (mounting options) of all removable media partitions. Look for entries that have mount points that contain words such as floppy or cdrom. See the **fstab(5)** manual page for more information.

#### References:

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230304  
Rule ID: SV-230304r627750  
STIG ID: RHEL-08-010610  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                      | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>2.3 <u>Address Unauthorized Software</u></b><br>Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently. |  |  |  |
| v7               | <b>2.6 <u>Address unapproved software</u></b><br>Ensure that unauthorized software is either removed or the inventory is updated in a timely manner                                                          |  |  |  |

### *1.1.2.12 Ensure all non-root local partitions are mounted with the "nodev" option (Automated)*

**Profile Applicability:**

- STIG

**Description:**

The operating system must prevent special devices on non-root local partitions.

**Rationale:**

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access. The only legitimate location for device files is the "/dev" directory located on the root partition.

**Audit:**

Verify all non-root local partitions are mounted with the "nodev" option with the following command:

```
# mount | grep '^/dev\S* on /\S' | grep --invert-match 'nodev'
```

If any output is produced, this is a finding.

**Remediation:**

Configure the "/etc/fstab" to use the "nodev" option on all non-root local partitions.

**References:**

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230301  
Rule ID: SV-230301r627750  
STIG ID: RHEL-08-010580  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |



### 1.1.3 Configure disk encryption

Linux Unified Key Setup (LUKS) is the standard for Linux hard disk encryption.

**Important** LUKS is not recommended for the following scenarios:

- Disk-encryption solutions such as LUKS protect the data only when your system is off. After the system is on and LUKS has decrypted the disk, the files on that disk are available to anyone who have access to them.
- Scenarios that require multiple users to have distinct access keys to the same device. The LUKS1 format provides eight key slots and LUKS2 provides up to 32 key slots.
- Applications that require file-level encryption.

### 1.1.3.1 Ensure all information at rest is encrypted (Manual)

#### Profile Applicability:

- STIG

#### Description:

Linux Unified Key Setup-on-disk-format (LUKS) provides a set of tools that simplifies managing the encrypted devices. With LUKS, you can encrypt block devices and enable multiple user keys to decrypt a master key. For bulk encryption of the partition, use this master key.

Red Hat Enterprise Linux uses LUKS to perform block device encryption. By default, the option to encrypt the block device is unchecked during the installation. If you select the option to encrypt your disk, the system prompts you for a passphrase every time you boot the computer. This passphrase unlocks the bulk encryption key that decrypts your partition. If you want to modify the default partition table, you can select the partitions that you want to encrypt. This is set in the partition table settings.

The default cipher used for LUKS is **aes-xts-plain64**. The default key size for LUKS is **512 bits**. The default key size for LUKS with Anaconda XTS mode is **512 bits**.

The following are the available ciphers:

- Advanced Encryption Standard (AES)
- Twofish
- Serpent

#### Rationale:

Systems handling data requiring "data at rest" protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest.

Selection of a cryptographic mechanism is based on the need to protect the integrity of organizational information. The strength of the mechanism is commensurate with the security category and/or classification of the information. Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields).

Satisfies: SRG-OS-000185-GPOS-00079, SRG-OS-000404-GPOS-00183, SRG-OS-000405-GPOS-00184

**Note:** Data in transit isn't protected, so data shared between devices and through email is still vulnerable to hacking.

**Impact:**

If users forget their password and lose their recovery key, the device will be inaccessible to them, and they will be locked out just like an intruder.

**Audit:**

Verify the operating system prevents unauthorized disclosure or modification of all information requiring at-rest protection by using disk encryption.

Verify with the following command:

Run the following command to verify all system partitions are encrypted:

```
# blkid
```

Verify every persistent disk partition present is type **crypto\_LUKS**

*Example output:*

```
/dev/mapper/rhel-root: UUID="67b7d7fe-de60-6fd0-befb-e6748cf97743"  
TYPE="crypto_LUKS"
```

Every persistent disk partition present must be of type "crypto\_LUKS". If any partitions other than pseudo file systems (such as /proc or /sys) are not type "crypto\_LUKS", ask the administrator to indicate how the partitions are encrypted. If there is no evidence that all local disk partitions are encrypted, this is a finding.

**Note:** If there is a documented and approved reason for not having data-at-rest encryption, this Recommendation is Not Applicable.

**Remediation:**

Configure the operating system to prevent unauthorized modification of all information at rest by using disk encryption.

Encrypting a partition in an already installed system is more difficult, because existing partitions will need to be resized and changed. To encrypt an entire partition, dedicate a partition for encryption in the partition layout.

**References:**

1. NIST SP 800-53 :: SC-28
2. NIST SP 800-53A :: SC-28.1

## Additional Information:

### Red Hat Enterprise Linux 8

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230224  
RULE ID: SV-230224r917864  
STIG ID: RHEL-08-010030  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | IG 1 | IG 2 | IG 3 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.11 <u>Encrypt Sensitive Data at Rest</u></b><br>Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data. |      | ●    | ●    |
| v7               | <b>14.8 <u>Encrypt Sensitive Information at Rest</u></b><br>Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.                                                                                                                                                                                                                             |      |      | ●    |

## 1.2 Package Management

Patch management procedures may vary widely between enterprises. Large enterprises may choose to install a local updates server that can be used in place of their distributions servers, whereas a single deployment of a system may prefer to get updates directly. Updates can be performed automatically or manually, depending on the site's policy for patch management. Organizations may prefer to test patches against their environment on a non-production system before rolling out to production.

Outdated software is vulnerable to cyber criminals and hackers. Software updates help reduce the risk to your organization. The release of software update notes often reveal the patched exploitable entry points to the public. Public knowledge of these exploits can make your organization more vulnerable to malicious actors attempting to gain entry to your system's data.

Software updates often offer new and improved features and speed enhancements

For the purpose of this benchmark, the requirement is to ensure that a patch management process is defined and maintained, the specifics of which are left to the organization.

## 1.2.1 Configure Package Repositories

Patch management procedures may vary widely between enterprises. Large enterprises may choose to install a local updates server that can be used in place of their distributions servers, whereas a single deployment of a system may prefer to get updates directly. Updates can be performed automatically or manually, depending on the site's policy for patch management. Organizations may prefer to test patches against their environment on a non-production system before rolling out to production.

Outdated software is vulnerable to cyber criminals and hackers. Software updates help reduce the risk to your organization. The release of software update notes often reveals the patched exploitable entry points to the public. Public knowledge of these exploits can leave your organization more vulnerable to malicious actors attempting to gain access to your system's data.

**Note:** Creation of an appropriate patch management policy is left to the organization.

### 1.2.1.1 Ensure GPG keys are configured (Manual)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The RPM Package Manager implements GPG key signing to verify package integrity during and after installation.

#### Rationale:

It is important to ensure that updates are obtained from a valid source to protect against spoofing that could lead to the inadvertent installation of malware on the system. To this end, verify that GPG keys are configured correctly for your system.

#### Audit:

##### List all GPG key URLs

Each repository should have a **gpgkey** with a URL pointing to the location of the GPG key, either local or remote.

```
# grep -r gpgkey /etc/yum.repos.d/* /etc/dnf/dnf.conf
```

##### List installed GPG keys

Run the following command to list the currently installed keys. These are the active keys used for verification and installation of RPMs. The packages are fake, they are generated on the fly by **dnf** or **rpm** during the import of keys from the URL specified in the repository configuration.

*Example:*

```
# for RPM_PACKAGE in $(rpm -q gpg-pubkey); do
  echo "RPM: ${RPM_PACKAGE}"
  RPM_SUMMARY=$(rpm -q --queryformat "%{SUMMARY}" "${RPM_PACKAGE}")
  RPM_PACKAGER=$(rpm -q --queryformat "%{PACKAGER}" "${RPM_PACKAGE}")
  RPM_DATE=$(date +%Y-%m-%d -d "1970-1-1+${((0x$(rpm -q --queryformat
"%{RELEASE}" "${RPM_PACKAGE}"))))sec")
  RPM_KEY_ID=$(rpm -q --queryformat "%{VERSION}" "${RPM_PACKAGE}")
  echo "Packager: ${RPM_PACKAGER}
Summary: ${RPM_SUMMARY}
Creation date: ${RPM_DATE}
Key ID: ${RPM_KEY_ID}
"
done

RPM: gpg-pubkey-9db62fb1-59920156
Packager: Fedora 28 (28) <fedora-28@fedoraproject.org>
Summary: gpg(Fedora 28 (28) <fedora-28@fedoraproject.org>)
Creation date: 2017-08-14
Key ID: 9db62fb1

RPM: gpg-pubkey-09eab3f2-595fbba3
Packager: RPM Fusion free repository for Fedora (28) <rpmfusion-
buildsys@lists.rpmfusion.org>
Summary: gpg(RPM Fusion free repository for Fedora (28) <rpmfusion-
buildsys@lists.rpmfusion.org>)
Creation date: 2017-07-07
Key ID: 09eab3f2
```

The format of the package (**gpg-pubkey-9db62fb1-59920156**) is important to understand for verification. Using the above example, it consists of three parts:

1. The general prefix name for all imported GPG keys: **gpg-pubkey-**
2. The version, which is the GPG key ID: **9db62fb1**
3. The release is the date of the key in UNIX timestamp in hexadecimal: **59920156**

With both the date and the GPG key ID, check the relevant repositories public key page to confirm that the keys are indeed correct.

### Query locally available GPG keys

Repositories that store their respective GPG keys on disk should do so in **/etc/pki/rpm-gpg/**. These keys are available for immediate import either when **dnf** is asked to install a relevant package from the repository or when an administrator imports the key directly with the **rpm --import** command.

To find where these keys come from run:

```
# for PACKAGE in $(find /etc/pki/rpm-gpg/ -type f -exec rpm -qf {} \; | sort
-u); do rpm -q --queryformat "%{NAME}-%{VERSION} %{PACKAGER} %{SUMMARY}\\n"
"${PACKAGE}"; done
```

### Remediation:

Update your package manager GPG keys in accordance with site policy.



## References:

1. NIST SP 800-53 Rev. 5: SI-2

## Additional Information:

Fedora public keys: <https://getfedora.org/security/>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b><u>7.3 Perform Automated Operating System Patch Management</u></b><br>Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.                                              |    |    |    |
| v8               | <b><u>7.4 Perform Automated Application Patch Management</u></b><br>Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.                                                        |    |    |    |
| v7               | <b><u>3.4 Deploy Automated Operating System Patch Management Tools</u></b><br>Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.      |  |  |  |
| v7               | <b><u>3.5 Deploy Automated Software Patch Management Tools</u></b><br>Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1195, T1195.001, T1195.002 | TA0001  | M1051       |

### 1.2.1.2 Ensure *gpgcheck* is globally activated (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The **gpgcheck** option, found in the main section of the **/etc/dnf/dnf.conf** and individual **/etc/yum.repos.d/\*** files, determines if an RPM package's signature is checked prior to its installation.

#### Rationale:

It is important to ensure that an RPM's package signature is always checked prior to installation to ensure that the software is obtained from a trusted source.

#### Audit:

Global configuration. Run the following command and verify that global configuration for **gpgcheck** is enabled. (set to **1**, **True**, or **yes**):

```
# grep -Pi -- '^h*gpgcheck\h*=\h*(1|true|yes)\b' /etc/dnf/dnf.conf
gpgcheck=1
```

**Note:** **true** or **yes** is also acceptable

Configuration in **/etc/yum.repos.d/** takes precedence over the global configuration.

Run the following command and verify that there are no instances of entries starting with **gpgcheck** returned set to **0**. Nor should there be any invalid (non-boolean) values. When **dnf** encounters such invalid entries they are ignored and the global configuration is applied.

```
# grep -Pris -- '^h*gpgcheck\h*=\h*(0|[2-9]|[1-9][0-9]+|false|no)\b' /etc/yum.repos.d/
```

Nothing should be returned

## Remediation:

Edit `/etc/dnf/dnf.conf` and set `gpgcheck=1`:

*Example*

```
# sed -i 's/^gpgcheck\s*=\s*\.*/gpgcheck=1/' /etc/dnf/dnf.conf
```

Edit any failing files in `/etc/yum.repos.d/*` and set all instances starting with `gpgcheck` to `1`.

*Example:*

```
# find /etc/yum.repos.d/ -name "*.repo" -exec echo "Checking:" {} \; -exec  
sed -i 's/^gpgcheck\s*=\s*\.*/gpgcheck=1/' {} \;
```

## References:

1. NIST SP 800-53 Rev. 5: SI-2

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230264  
Rule ID: SV-230264r880711  
STIG ID: RHEL-08-010370  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                          | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>7.3 <u>Perform Automated Operating System Patch Management</u></b><br>Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.                                         |  |  |  |
| v7               | <b>3.4 <u>Deploy Automated Operating System Patch Management Tools</u></b><br>Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor. |  |  |  |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1195, T1195.001                   | TA0005         |                    |

### 1.2.1.3 Ensure repo\_gpgcheck is globally activated (Manual)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

#### Description:

The `repo_gpgcheck` option, found in the main section of the `/etc/dnf/dnf.conf` and individual `/etc/yum.repos.d/*` files, will perform a GPG signature check on the repodata.

#### Rationale:

It is important to ensure that the repository data signature is always checked prior to installation to ensure that the software is not tampered with in any way.

#### Impact:

Not all repositories, notably RedHat, support `repo_gpgcheck`. Take care to set this value to false (default) for particular repositories that do not support it. If enabled on repositories that do not support `repo_gpgcheck` installation of packages will fail.

Research is required by the user to determine which repositories is configured on the local system and, from that list, which support `repo_gpgcheck`.

#### Audit:

#### Global configuration

Run the following command:

```
grep ^repo_gpgcheck /etc/dnf/dnf.conf
```

Verify that `repo_gpgcheck` is set to **1**

#### Per repository configuration

Configuration in `/etc/yum.repos.d/` takes precedence over the global configuration.

As an example, to list all the configured repositories, excluding "fedoraproject.org", that specifically disables `repo_gpgcheck`, run the following command:

```
# REPO_URL="fedoraproject.org"
# for repo in $(grep -l "repo_gpgcheck=0" /etc/yum.repos.d/* ); do
  if ! grep "${REPO_URL}" "${repo}" &>/dev/null; then
    echo "${repo}"
  fi
done
```

Per the research that was done on which repositories does not support `repo_gpgcheck`, change the `REPO_URL` variable and run the test.

## Remediation:

### Global configuration

Edit `/etc/dnf/dnf.conf` and set `repo_gpgcheck=1` in the `[main]` section.

Example:

```
[main]
repo_gpgcheck=1
```

### Per repository configuration

First check that the particular repository support GPG checking on the repodata.

Edit any failing files in `/etc/yum.repos.d/*` and set all instances starting with `repo_gpgcheck` to `1`.

## References:

1. NIST SP 800-53 Rev. 5: SI-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                          | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>7.3 <u>Perform Automated Operating System Patch Management</u></b><br>Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.                                         |  |  |  |
| v7               | <b>3.4 <u>Deploy Automated Operating System Patch Management Tools</u></b><br>Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1195, T1195.001            | TA0005  |             |

### 1.2.1.4 Ensure package manager repositories are configured (Manual)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

Systems need to have the respective package manager repositories configured to ensure that the system is able to receive the latest patches and updates.

#### Rationale:

If a system's package repositories are misconfigured, important patches may not be identified or a rogue repository could introduce compromised software.

#### Audit:

Run the following command to verify repositories are configured correctly. The output may vary depending on which repositories are currently configured on the system.

*Example:*

```
# dnf repolist
Last metadata expiration check: 1:00:00 ago on Mon 1 Jan 2021 00:00:00 BST.
repo id      repo name      status
*fedora      Fedora 28 - x86_64  57,327
*updates     Fedora 28 - x86_64 - Updates 22,133
```

For the repositories in use, inspect the configuration file to ensure all settings are correctly applied according to site policy.

*Example:*

Depending on the distribution being used the repo file name might differ.

```
cat /etc/yum.repos.d/*.repo
```

#### Remediation:

Configure your package manager repositories according to site policy.

#### References:

1. NIST SP 800-53 Rev. 5: SI-2

#### Additional Information:

For further information about Fedora repositories see: <https://docs.fedoraproject.org/en-US/quick-docs/repositories/>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>7.3 Perform Automated Operating System Patch Management</u></b><br>Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.                                              |  |  |  |
| v8               | <b><u>7.4 Perform Automated Application Patch Management</u></b><br>Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.                                                        |  |  |  |
| v7               | <b><u>3.4 Deploy Automated Operating System Patch Management Tools</u></b><br>Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.      |  |  |  |
| v7               | <b><u>3.5 Deploy Automated Software Patch Management Tools</u></b><br>Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1195, T1195.001            | TA0001  | M1051       |



### *1.2.1.5 Ensure DNF is configured to perform a signature check on local packages (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components of local packages without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.

#### **Rationale:**

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved CA.

#### **Audit:**

Verify the operating system prevents the installation of patches, service packs, device drivers, or operating system components from a repository without verification that they have been digitally signed using a certificate that is recognized and approved by the organization.

Check if DNF is configured to perform a signature check on local packages with the following command:

```
# grep -i localpkg_gpgcheck /etc/dnf/dnf.conf  
localpkg_gpgcheck =True
```

If "localpkg\_gpgcheck" is not set to either "1", "True", or "yes", commented out, or is missing from "/etc/dnf/dnf.conf", this is a finding.

## Remediation:

Configure the operating system to remove all software components after updated versions have been installed.

Set the "localpkg\_gpgcheck" option to "True" in the "/etc/dnf/dnf.conf" file:

```
localpkg_gpgcheck=True
```

## References:

1. NIST SP 800-53 Revision 4 :: CM-5 (3)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230265  
Rule ID: SV-230265r877463  
STIG ID: RHEL-08-010371  
Severity: CAT I

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b><u>7.3 Perform Automated Operating System Patch Management</u></b><br>Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.                                              |  |  |  |
| v8               | <b><u>7.4 Perform Automated Application Patch Management</u></b><br>Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.                                                        |  |  |  |
| v7               | <b><u>3.4 Deploy Automated Operating System Patch Management Tools</u></b><br>Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.      |  |  |  |
| v7               | <b><u>3.5 Deploy Automated Software Patch Management Tools</u></b><br>Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor. |  |  |  |

## 1.2.1.6 Ensure cryptographic verification of vendor software packages (Manual)

### Profile Applicability:

- STIG

### Description:

Red Hat cryptographically signs all software packages, which includes updates, with a GPG key to verify that they are valid.

### Rationale:

Cryptographic verification of vendor software packages ensures that all software packages are obtained from a valid source and protects against spoofing that could lead to installation of malware on the system

### Audit:

Run the following commands and verify Red Hat package-signing keys are installed on the system and their fingerprints match vendor values:

**Note:** For RHEL 8 software packages, Red Hat uses GPG keys labeled **release key 2** and **auxiliary key 2**. The keys are defined in key file **/etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release** by default.

List Red Hat GPG keys installed on the system:

```
# rpm -q --queryformat "%{SUMMARY}\n" gpg-pubkey | grep -i "red hat"

gpg(Red Hat, Inc. (release key 2) <security@redhat.com>)
gpg(Red Hat, Inc. (auxiliary key) <security@redhat.com>)
```

**Note:** The "auxiliary key 2**appears as** auxiliary key` on a RHEL 8 system.  
List key fingerprints of installed Red Hat GPG keys:

```
# sudo gpg -q --keyid-format short --with-fingerprint /etc/pki/rpm-gpg/RPM-
GPG-KEY-redhat-release
```

### Example output:

```
pub  rsa4096/FD431D51 2009-10-22 [SC]
    Key fingerprint = 567E 347A D004 4ADE 55BA  8A5F 199E 2F91 FD43 1D51
uid                               Red Hat, Inc. (release key 2) <security@redhat.com>
pub  rsa4096/D4082792 2018-06-27 [SC]
    Key fingerprint = 6A6A A7C9 7C88 90AE C6AE  BFE2 F76F 66C3 D408 2792
uid                               Red Hat, Inc. (auxiliary key) <security@redhat.com>
sub  rsa4096/1B5584D3 2018-06-27 [E]
```

Compare key fingerprints of installed Red Hat GPG keys with fingerprints listed for RHEL 8 on Red Hat "Product Signing Keys" webpage at <https://access.redhat.com/security/team/key>.

## Remediation:

Install Red Hat package-signing keys on the system and verify their fingerprints match vendor values.

Insert RHEL 8 installation disc or attach RHEL 8 installation image to the system. Mount the disc or image to make the contents accessible inside the system.

Assuming the mounted location is `/media/cdrom`, use the following command to copy Red Hat GPG key file onto the system:

```
# cp /media/cdrom/RPM-GPG-KEY-redhat-release /etc/pki/rpm-gpg/
```

Import Red Hat GPG keys from key file into system keyring:

```
# rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

## References:

1. NIST SP 800-53 Revision 4 :: CM-5 (3)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-256973  
Rule ID: SV-256973r902752  
STIG ID: RHEL-08-010019  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

## 1.2.2 Configure Package Updates

### *1.2.2.1 Ensure updates, patches, and additional security software are installed (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Periodically patches are released for included software either due to security flaws or to include additional functionality.

#### **Rationale:**

Newer patches may contain security enhancements that would not be available through the latest full update. As a result, it is recommended that the latest software patches be used to take advantage of the latest functionality. As with any software installation, organizations need to determine if a given update meets their requirements and verify the compatibility and supportability of any additional software against the update revision that is selected.

#### **Audit:**

Run the following command and verify there are no updates or patches to install:

```
# dnf check-update
```

Check to make sure no system reboot is required

```
dnf needs-restarting -r
```

#### **Remediation:**

Use your package manager to update all packages on the system according to site policy.

The following command will install all available updates:

```
# dnf update
```

Once the update process is complete, verify if reboot is required to load changes.

```
dnf needs-restarting -r
```

#### **References:**

1. NIST SP 800-53 Rev. 5: SI-2

## Additional Information:

Site policy may mandate a testing period before installation of available updates onto production systems.

```
# dnf check-update
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>7.3 <u>Perform Automated Operating System Patch Management</u></b><br>Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.                                              |    |    |    |
| v8               | <b>7.4 <u>Perform Automated Application Patch Management</u></b><br>Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.                                                        |    |    |    |
| v7               | <b>3.4 <u>Deploy Automated Operating System Patch Management Tools</u></b><br>Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.      |    |    |    |
| v7               | <b>3.5 <u>Deploy Automated Software Patch Management Tools</u></b><br>Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics        | Mitigations |
|-----------------------------|----------------|-------------|
| T1211, T1211.000            | TA0004, TA0008 | M1051       |

## 1.2.2.2 Ensure vendor packaged system security patches and updates are installed (Manual)

### Profile Applicability:

- STIG

### Description:

Patches are released for included software either due to security flaws or to include additional functionality.

### Rationale:

Timely patching is critical for maintaining the operational availability, confidentiality, and integrity of information technology (IT) systems. New patches are released frequently, and it is often difficult to keep abreast of all the new patches. When new weaknesses in an operating system exist, patches are usually made available by the vendor to resolve the problems. If the most recent security patches and updates are not installed, unauthorized users may take advantage of weaknesses in the unpatched software. The lack of prompt attention to patching could result in a system compromise.

### Audit:

Run the following command and verify the operating system security patches and updates are installed and up to date:

```
# dnf history list | more
```

### Example output:

```
Updating Subscription Management repositories.
ID      | Command line                                | Date and time      |
Action(s) | Altered
-----|-----
4 | update                                | 2024-08-28 14:18 |
Upgrade | 25
3 | update                                | 2024-08-20 08:28 |
Upgrade | 9
2 | update                                | 2024-08-16 11:56 |
I, O, U | 940 EE
1 |                                         | 2024-08-16 11:38 |
Install | 1376 EE
```

Verify package updates have been performed on the system within the timeframe dictated by site policy

**Note:** Typical update frequency may be overridden by a discovered vulnerability. e.g. Information Assurance Vulnerability Alert (IAVA) notifications from CYBERCOM or a Common Vulnerabilities and Exposures (CVE).



## Remediation:

Use your package manager to update all packages on the system according to site policy.

The following command will install all available updates:

```
# dnf update
```

Once the update process is complete, verify if reboot is required to load changes.

```
dnf needs-restarting -r
```

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Site policy may mandate a testing period before installation of available updates onto production systems.

```
# dnf check-update
```

### Red Hat Enterprise Linux 8

```
Red Hat Enterprise Linux 8
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230222
RULE ID: SV-230222r627750
STIG ID: RHEL-08-010010
SEVERITY: CAT II
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>7.3 Perform Automated Operating System Patch Management</u></b><br>Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.                                              |  |  |  |
| v8               | <b><u>7.4 Perform Automated Application Patch Management</u></b><br>Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.                                                        |  |  |  |
| v7               | <b><u>3.4 Deploy Automated Operating System Patch Management Tools</u></b><br>Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.      |  |  |  |
| v7               | <b><u>3.5 Deploy Automated Software Patch Management Tools</u></b><br>Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics        | Mitigations |
|-----------------------------|----------------|-------------|
| T1211, T1211.000            | TA0004, TA0008 | M1051       |

### 1.2.2.3 Ensure Operating System is a vendor-supported release (Manual)

#### Profile Applicability:

- STIG

#### Description:

An operating system release is considered "supported" if the vendor continues to provide security patches for the product

#### Rationale:

With an unsupported release, it will not be possible to resolve security issues discovered in the system software.

#### Audit:

Run the following command to verify the version of the operation system:

```
# grep -i version_id /etc/os-release
```

*Example output:*

```
VERSION_ID="8.10"
```

Verify that the version listed is still supported by the vendor

#### Remediation:

Upgrade to a supported version of the Operating System (OS)

Run the following command to install the latest patches:

```
# dnf update
```

#### References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)
3. <https://access.redhat.com/support/policy/updates/errata/>

#### Additional Information:

Red Hat Enterprise Linux 8

```
Red Hat Enterprise Linux 8
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230221
RULE ID: SV-230221r858734
STIG ID: RHEL-08-010000
SEVERITY: CAT I
```

### *1.2.2.4 Ensure the operating system removes all software components after updated versions have been installed (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

DNF must remove all software components after updated versions have been installed on the operating system.

#### **Rationale:**

Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software automatically from the information system.

#### **Audit:**

Verify the operating system removes all software components after updated versions have been installed.

Check if DNF is configured to remove unneeded packages with the following command:

```
# grep -i clean_requirements_on_remove /etc/dnf/dnf.conf  
  
clean_requirements_on_remove=True
```

If "clean\_requirements\_on\_remove" is not set to either "1", "True", or "yes", commented out, or is missing from "/etc/dnf/dnf.conf", this is a finding.

#### **Remediation:**

Configure the operating system to remove all software components after updated versions have been installed.

Set the "clean\_requirements\_on\_remove" option to "True" in the "/etc/dnf/dnf.conf" file:

```
clean_requirements_on_remove=True
```

#### **References:**

1. NIST SP 800-53 Revision 5 :: SI-2 (6)

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230281  
Rule ID: SV-230281r854034  
STIG ID: RHEL-08-010440  
Severity: CAT III

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

## 1.3 Mandatory Access Control

Mandatory Access Control (MAC) provides an additional layer of access restrictions to processes on top of the base Discretionary Access Controls. By restricting how processes can access files and resources on a system the potential impact from vulnerabilities in the processes can be reduced.

**Impact:** Mandatory Access Control limits the capabilities of applications and daemons on a system, while this can prevent unauthorized access the configuration of MAC can be complex and difficult to implement correctly preventing legitimate access from occurring.

### 1.3.1 Configure SELinux

SELinux implements Mandatory Access Control (MAC). Every process and system resource has a special security label called an SELinux context. A SELinux context, sometimes referred to as an SELinux label, is an identifier which abstracts away the system-level details and focuses on the security properties of the entity. Not only does this provide a consistent way of referencing objects in the SELinux policy, but it also removes any ambiguity that can be found in other identification methods. For example, a file can have multiple valid path names on a system that makes use of bind mounts.

The SELinux policy uses these contexts in a series of rules which define how processes can interact with each other and the various system resources. By default, the policy does not allow any interaction unless a rule explicitly grants access.

In Fedora 28 Family Linux distributions, system services are controlled by the `systemd` daemon; `systemd` starts and stops all services, and users and processes communicate with `systemd` using the `systemctl` utility. The `systemd` daemon can consult the SELinux policy and check the label of the calling process and the label of the unit file that the caller tries to manage, and then ask SELinux whether or not the caller is allowed the access. This approach strengthens access control to critical system capabilities, which include starting and stopping system services.

This automatically limits the damage that the software can do to files accessible by the calling user. The user does not need to take any action to gain this benefit. For an action to occur, both the traditional DAC permissions must be satisfied as well as the SELinux MAC rules. The action will not be allowed if either one of these models does not permit the action. In this way, SELinux rules can only make a system's permissions more restrictive and secure. SELinux requires a complex policy to allow all the actions required of a system under normal operation.

Two such policies have been designed for use with Fedora 28 Family Linux distributions and are included with the system:

- **targeted** - Targeted processes run in their own domain, called a confined domain. In a confined domain, the files that a targeted process has access to are limited. If a confined process is compromised by an attacker, the attacker's access to resources and the possible damage they can do is also limited. SELinux denies access to these resources and logs the denial.
- **mls** - Implements Multi-Level Security (MLS), which introduces even more kinds of labels (sensitivity and category) and rules that govern access based on these.

This section provides guidance for the configuration of the **targeted** policy.

**Note:**

- Remember that SELinux policy rules are checked after DAC rules. SELinux policy rules are not used if DAC rules deny access first, which means that no SELinux denial is logged if the traditional DAC rules prevent the access.
- This section only applies if SELinux is in use on the system. Additional Mandatory Access Control systems exist.
- To avoid incorrect SELinux labeling and subsequent problems, ensure that you start services using a `systemctl start` command.

**References:**

- NSA SELinux resources:
  - <https://www.nsa.gov/Research/Technical-Papers-Brochures/smdsearch14229/selinux>
- Fedora SELinux resources:
  - Getting started with SELinux: <https://docs.fedoraproject.org/en-US/quick-docs/getting-started-with-selinux>
  - User Guide: [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/8/html-single/using\\_selinux/index](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html-single/using_selinux/index)
- SELinux Project web page and wiki:
  - <http://www.selinuxproject.org>



### 1.3.1.1 Ensure SELinux is installed (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

SELinux provides Mandatory Access Control.

#### Rationale:

Without a Mandatory Access Control system installed only the default Discretionary Access Control system will be available.

#### Audit:

Verify SELinux is installed.  
Run the following command:

```
# rpm -q libselinux  
  
libselinux-<version>
```

#### Remediation:

Run the following command to install **SELinux**:

```
# dnf install libselinux
```

#### References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

#### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1068, T1068.000                   | TA0003         | M1026              |

### *1.3.1.2 Ensure SELinux is not disabled in bootloader configuration (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Configure SELINUX to be enabled at boot time and verify that it has not been overwritten by the grub boot parameters.

#### **Rationale:**

SELinux must be enabled at boot time in your grub configuration to ensure that the controls it provides are not overridden.

#### **Impact:**

Files created while SELinux is disabled are not labeled at all. This behavior causes problems when changing to enforcing mode because files are labeled incorrectly or are not labeled at all. To prevent incorrectly labeled and unlabeled files from causing problems, file systems are automatically relabeled when changing from the disabled state to permissive or enforcing mode. This can be a long running process that should be accounted for as it may extend downtime during initial re-boot.

#### **Audit:**

Run the following command to verify that neither the **selinux=0** or **enforcing=0** parameters have been set:

```
# grubby --info=ALL | grep -Po '(selinux|enforcing)=0\b'
```

Nothing should be returned

## Remediation:

Run the following command to remove the **selinux=0** and **enforcing=0** parameters:

```
grubby --update-kernel ALL --remove-args "selinux=0 enforcing=0"
```

Run the following command to remove the **selinux=0** and **enforcing=0** parameters if they were created by the deprecated **grub2-mkconfig** command:

```
# grep -Prsq --
'\h*([\#\n\r]+\h+)?kernelopts=([\#\n\r]+\h+)?(selinux|enforcing)=0\b'
/boot/grub2 /boot/efi && grub2-mkconfig -o "$(grep -Pr1 --
'\h*([\#\n\r]+\h+)?kernelopts=([\#\n\r]+\h+)?(selinux|enforcing)=0\b'
/boot/grub2 /boot/efi) "
```

## References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## Additional Information:

This recommendation is designed around the grub 2 bootloader, if another bootloader is in use in your environment enact equivalent settings.

**grubby** is a command line tool for updating and displaying information about the configuration files for the grub2 and zipl boot loaders. It is primarily designed to be used from scripts which install new kernels and need to find information about the current boot environment.

- All bootloaders define the boot entries as individual configuration fragments that are stored by default in **/boot/loader/entries**. The format for the config files is specified at [https://systemd.io/BOOT\\_LOADER\\_SPECIFICATION](https://systemd.io/BOOT_LOADER_SPECIFICATION). The grubby tool is used to update and display the configuration defined in the **BootLoaderSpec** fragment files.
- There are a number of ways to specify the kernel used for --info, --remove-kernel, and --update-kernel. Specifying DEFAULT or ALL selects the de-fault entry and all of the entries, respectively. Also, the title of a boot entry may be specified by using TITLE=title as the argument; all entries with that title are used.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1068, T1068.000            | TA0003  | M1026       |

### 1.3.1.3 Ensure SELinux policy is configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

Configure SELinux to meet or exceed the default targeted policy, which constrains daemons and system software only.

#### Rationale:

Security configuration requirements vary from site to site. Some sites may mandate a policy that is stricter than the default policy, which is perfectly acceptable. This item is intended to ensure that at least the default recommendations are met.

#### Audit:

Run the following commands and ensure output matches either " **targeted** " or " **mls** ":

```
# grep -E '^s*SELINUXTYPE=(targeted|mls)\b' /etc/selinux/config
SELINUXTYPE=targeted
# sestatus | grep Loaded
Loaded policy name:           targeted
```

#### Remediation:

Edit the **/etc/selinux/config** file to set the SELINUXTYPE parameter:

```
SELINUXTYPE=targeted
```

#### References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

#### Additional Information:

If your organization requires stricter policies, ensure that they are set in the **/etc/selinux/config** file.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1068, T1068.000            | TA0005  |             |

### 1.3.1.4 Ensure the SELinux mode is not disabled (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

SELinux can run in one of three modes: disabled, permissive, or enforcing:

- **Enforcing** - Is the default, and recommended, mode of operation; in enforcing mode SELinux operates normally, enforcing the loaded security policy on the entire system.
- **Permissive** - The system acts as if SELinux is enforcing the loaded security policy, including labeling objects and emitting access denial entries in the logs, but it does not actually deny any operations. While not recommended for production systems, permissive mode can be helpful for SELinux policy development.
- **Disabled** - Is strongly discouraged; not only does the system avoid enforcing the SELinux policy, it also avoids labeling any persistent objects such as files, making it difficult to enable SELinux in the future

**Note:** You can set individual domains to permissive mode while the system runs in enforcing mode. For example, to make the httpd\_t domain permissive:

```
# semanage permissive -a httpd_t
```

#### Rationale:

Running SELinux in disabled mode is strongly discouraged; not only does the system avoid enforcing the SELinux policy, it also avoids labeling any persistent objects such as files, making it difficult to enable SELinux in the future.



## Audit:

Run the following command to verify SELinux's current mode:

```
# getenforce  
  
Enforcing  
-OR-  
Permissive
```

Run the following command to verify SELinux's configured mode:

```
# grep -Ei '^s*SELINUX=(enforcing|permissive)' /etc/selinux/config  
  
SELINUX=enforcing  
-OR-  
SELINUX=permissive
```

## Remediation:

Run one of the following commands to set SELinux's running mode:

To set SELinux mode to **Enforcing**:

```
# setenforce 1
```

**- OR -**

To set SELinux mode to **Permissive**:

```
# setenforce 0
```

Edit the **/etc/selinux/config** file to set the SELINUX parameter:

For Enforcing mode:

```
SELINUX=enforcing
```

**- OR -**

For Permissive mode:

```
SELINUX=permissive
```

## References:

1. [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/7/html/selinux\\_users\\_and\\_administrators\\_guide/sect-security-enhanced\\_linux-introduction-selinux\\_modes](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/sect-security-enhanced_linux-introduction-selinux_modes)
2. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques                   | Tactics | Mitigations |
|-----------------------------------------------|---------|-------------|
| T1068, T1068.000, T1565, T1565.001, T1565.003 | TA0003  | M1026       |

### 1.3.1.5 Ensure the SELinux mode is enforcing (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### Description:

SELinux can run in one of three modes: disabled, permissive, or enforcing:

- **Enforcing** - Is the default, and recommended, mode of operation; in enforcing mode SELinux operates normally, enforcing the loaded security policy on the entire system.
- **Permissive** - The system acts as if SELinux is enforcing the loaded security policy, including labeling objects and emitting access denial entries in the logs, but it does not actually deny any operations. While not recommended for production systems, permissive mode can be helpful for SELinux policy development.
- **Disabled** - Is strongly discouraged; not only does the system avoid enforcing the SELinux policy, it also avoids labeling any persistent objects such as files, making it difficult to enable SELinux in the future

**Note:** You can set individual domains to permissive mode while the system runs in enforcing mode. For example, to make the httpd\_t domain permissive:

```
# semanage permissive -a httpd_t
```

#### Rationale:

Running SELinux in disabled mode the system not only avoids enforcing the SELinux policy, it also avoids labeling any persistent objects such as files, making it difficult to enable SELinux in the future.

Running SELinux in Permissive mode, though helpful for developing SELinux policy, only logs access denial entries, but does not deny any operations.

#### Impact:

Running SELinux in Enforcing mode may block intended access to files or processes if the SELinux policy is not correctly configured. If this occurs, review the system logs for details and update labels or policy as appropriate.

## Audit:

Run the following command to verify SELinux's current mode:

```
# getenforce  
Enforcing
```

Run the following command to verify SELinux's configured mode:

```
# grep -i SELINUX=enforcing /etc/selinux/config  
SELINUX=enforcing
```

## Remediation:

Run the following command to set SELinux's running mode:

```
# setenforce 1
```

Edit the `/etc/selinux/config` file to set the SELINUX parameter:  
For Enforcing mode:

```
SELINUX=enforcing
```

## References:

1. [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/7/html/selinux\\_users\\_and\\_administrators\\_guide/sect-security-enhanced\\_linux-introduction-selinux\\_modes](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/sect-security-enhanced_linux-introduction-selinux_modes)
2. CCI-002165: The information system enforces organization-defined discretionary access control policies over defined subjects and objects.
3. NIST SP 800-53 Revision 4 :: AC-3 (4)
4. CCI-002696: The information system verifies correct operation of organization-defined security functions.
5. NIST SP 800-53 Revision 4 :: SI-6 a
6. NIST SP 800-53A :: SC-3.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230240  
Rule ID: SV-230240r627750  
STIG ID: RHEL-08-010170  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques                   | Tactics | Mitigations |
|-----------------------------------------------|---------|-------------|
| T1068, T1068.000, T1565, T1565.001, T1565.003 | TA0005  |             |

### *1.3.1.6 Ensure no unconfined services exist (Manual)*

**Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

**Description:**

Unconfined processes run in unconfined domains

**Rationale:**

For unconfined processes, SELinux policy rules are applied, but policy rules exist that allow processes running in unconfined domains almost all access. Processes running in unconfined domains fall back to using DAC rules exclusively. If an unconfined process is compromised, SELinux does not prevent an attacker from gaining access to system resources and data, but of course, DAC rules are still used. SELinux is a security enhancement on top of DAC rules – it does not replace them

**Impact:**

Confining a service that inherently requires unconfined access to function may disrupt its intended operations. This restriction may lead to downtime, degraded performance, or loss in functionality. It is crucial to analyze and adjust SELinux policies in accordance with site security policies and operational requirements.

**Audit:**

Run the following command and verify no output is produced:

```
# ps -eZ | grep unconfined_service_t
```

## Remediation:

Investigate any unconfined processes found during the audit action. If necessary, create a customized SELinux policy to allow necessary actions for the service.

**Warning:** Knowledge about creating and configuring SELinux policies is needed. A Basic example on how to create a policy is included below.

1. Identify the unconfined service: determine the name and process of the service
2. Identify the functionality: determine if the functionality is required for operations
3. Create or add to the custom allow list in the SELinux policy configuration

### *Example SELinux policy configuration: service\_allowlist\_policy.te*

```
# Example SELinux policy configuration for allowing access to specific
actions and resources for a service

module my_service 1.0;

require {
    type my_service_t;
    type system_resource_t;
    class file { read write execute };
    class dir { read write add_name };
    class tcp_socket name_connect;
}

allow my_service_t system_resource_t:file { read write execute }; # Allow
my_service_t to read, write, and execute files with the system_resource_t
context

allow my_service_t system_resource_t:dir { read write add_name }; # Allow
my_service_t to read and write to directories with the system_resource_t
context

allow my_service_t system_resource_t:tcp_socket name_connect; # Allow
my_service_t to establish TCP connections
```

#### 4. Compile the policy

```
# checkmodule -M -, -o service_allowlist_policy.mod
service_allowlist_policy.te
```

#### 5. Create the package

```
# semodule_package -o service_allowlist_policy.pp -m
service_allowlist_policy.mod
```

#### 6. Load the policy

```
# semodule -i service_allowlist_policy.pp
```

#### 7. Apply the policy to the service

```
# chcon -t se service_allowlist_policy /path/to/service_binary
```

## References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2
2. [https://nb.fedorapeople.org/cvsfedora/web/html/docs/selinux-guide/f10/en-US/sect-Security-Enhanced Linux-Targeted Policy-Unconfined Processes.html](https://nb.fedorapeople.org/cvsfedora/web/html/docs/selinux-guide/f10/en-US/sect-Security-Enhanced%20Linux-Targeted%20Policy-Unconfined%20Processes.html)
3. [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/9/html/using\\_selinux/managing-confined-and-unconfined-users\\_using-selinux](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/using_selinux/managing-confined-and-unconfined-users_using-selinux)
4. [https://access.redhat.com/documentation/id-red\\_hat\\_enterprise\\_linux/9/pdf/using\\_selinux/red\\_hat\\_enterprise\\_linux-9-using\\_selinux-en-us.pdf](https://access.redhat.com/documentation/id-red_hat_enterprise_linux/9/pdf/using_selinux/red_hat_enterprise_linux-9-using_selinux-en-us.pdf)

## Additional Information:

Occasionally certain daemons such as backup or centralized management software may require running unconfined. Any such software should be carefully analyzed and documented before such an exception is made.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                 | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |
| v7               | <b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                   |                                                                                       |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques                   | Tactics | Mitigations |
|-----------------------------------------------|---------|-------------|
| T1068, T1068.000, T1565, T1565.001, T1565.003 | TA0004  | M1022       |



### *1.3.1.7 Ensure the MCS Translation Service (mcstrans) is not installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `mcstransd` daemon provides category label information to client processes requesting information. The label translations are defined in `/etc/selinux/targeted/setrans.conf`

#### **Rationale:**

Since this service is not used very often, remove it to reduce the amount of potentially vulnerable code running on the system.

#### **Audit:**

Run the following command and verify `mcstrans` is not installed.

```
# rpm -q mcstrans  
package mcstrans is not installed
```

#### **Remediation:**

Run the following command to uninstall `mcstrans`:

```
# dnf remove mcstrans
```

#### **References:**

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1543, T1543.002            | TA0005  |             |

### *1.3.1.8 Ensure the operating system has the policycoreutils package installed (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must have the policycoreutils package installed.

#### **Rationale:**

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

Policycoreutils contains the policy core utilities that are required for basic operation of an SELinux-enabled system. These utilities include load\_policy to load SELinux policies, setfile to label filesystems, newrole to switch roles, and run\_init to run "/etc/init.d" scripts in the proper context.

#### **Audit:**

Verify the operating system has the policycoreutils package installed with the following command:

```
# dnf list installed policycoreutils  
policycoreutils.x86_64 2.9-3.el8 @anaconda
```

If the policycoreutils package is not installed, this is a finding.

#### **Remediation:**

Configure the operating system to have the policycoreutils package installed with the following command:

```
# dnf install policycoreutils
```

#### **References:**

1. NIST SP 800-53 Revision 5 :: SC-3
2. NIST SP 800-53A :: SC-3.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230241  
Rule ID: SV-230241r627750  
STIG ID: RHEL-08-010171  
Severity: CAT III

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### *1.3.1.9 Ensure SETroubleshoot is not installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server

#### **Description:**

The SETroubleshoot service notifies desktop users of SELinux denials through a user-friendly interface. The service provides important information around configuration errors, unauthorized intrusions, and other potential errors.

#### **Rationale:**

The SETroubleshoot service is an unnecessary daemon to have running on a server, especially if X Windows is disabled.

#### **Audit:**

Verify **setroubleshoot** is not installed.

Run the following command:

```
# rpm -q setroubleshoot  
package setroubleshoot is not installed
```

#### **Remediation:**

Run the following command to uninstall **setroubleshoot**:

```
# dnf remove setroubleshoot
```

#### **References:**

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.                                                                                                                                                    |                                                                                     |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1543, T1543.002            | TA0005  |             |

### 1.3.1.10 Ensure SELinux prevents nonprivileged users from executing privileged functions (Manual)

#### Profile Applicability:

- STIG

#### Description:

SELinux should be configured to prevent nonprivileged users from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards/countermeasures.

Privileged functions include, establishing accounts, performing system integrity checks, or administering cryptographic key management activities. Nonprivileged users are individuals who do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from nonprivileged users.

#### Rationale:

Preventing nonprivileged users from executing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

#### Audit:

Verify the operating system prevents nonprivileged users from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards/countermeasures by doing the following:

1. Obtain a list of authorized users (other than system administrator and guest accounts) for the system.
2. Check the list against the system by running the following command:

```
# sudo semanage login -l | more
```

#### Example Output:

| Login Name  | SELinux User | MLS/MCS Range  | Service |
|-------------|--------------|----------------|---------|
| __default__ | user_u       | s0-s0:c0.c1023 | *       |
| root        | unconfined_u | s0-s0:c0.c1023 | *       |
| system_u    | system_u     | s0-s0:c0.c1023 | *       |
| joe         | staff_u      | s0-s0:c0.c1023 | *       |

All administrators should be mapped to the **sysadm\_u**, **staff\_u**, or an appropriately tailored confined role as defined by the organization.

All authorized non-administrative users must be mapped to the **user\_u** role, or an appropriately tailored confined role as defined by the organization.

## Remediation:

Run the following commands to prevent nonprivileged users from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards/countermeasures:

Use the following command to map a new user to the **sysadm\_u** role:

```
# semanage login -a -s sysadm_u <username>
```

Use the following command to map an existing user to the **sysadm\_u** role:

```
# semanage login -m -s sysadm_u <username>
```

Use the following command to map a new user to the **staff\_u** role:

```
# semanage login -a -s staff_u <username>
```

Use the following command to map an existing user to the **staff\_u** role:

```
# semanage login -m -s staff_u <username>
```

Use the following command to map a new user to the **user\_u** role:

```
# semanage login -a -s user_u <username>
```

Use the following command to map an existing user to the **user\_u** role:

```
# semanage login -m -s user_u <username>
```

**Note:** SELinux confined users mapped to **sysadm\_u** are not allowed to log in to the system over SSH, by default. If this is a required function, it can be configured by setting the **ssh\_sysadm\_login** SELinux boolean to **on** with the following command:

```
# sudo setsebool -P ssh_sysadm_login on
```

## References:

1. NIST SP 800-53 Revision 5 :: AC-16 b



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-254520  
Rule ID: SV-254520r928805  
STIG ID: RHEL-08-040400  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### *1.3.1.11 Ensure SELinux targeted policy is configured (Manual)*

**Profile Applicability:**

- STIG

**Description:**

Configure SELinux to meet targeted policy, which constrains daemons and system software only.

**Rationale:**

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

## Audit:

Run the following command to verify SELinux is active and is enforcing the targeted policy:

```
# sestatus
```

### Example Output

```
SELinux status: enabled
SELinuxfs mount: /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policy name: targeted
Current mode: enforcing
Mode from config file: enforcing
Policy MLS status: enabled
Policy deny_unknown status: allowed
Memory protection checking: actual (secure)
Max kernel policy version: 31
```

**Note:** The output must include **Loaded policy name: targeted**  
Run the following command to verify that the **/etc/selinux/config** file is configured to the **SELINUXTYPE** to **targeted**:

```
# grep -i "selinuxtype" /etc/selinux/config | grep -v '^#'

SELINUXTYPE = targeted
```

## Remediation:

Configure the operating system to verify correct operation of all security functions.  
Set the **SELinuxtype** to the **targeted** policy by modifying the **/etc/selinux/config** file to have the following line:

```
SELINUXTYPE=targeted
```

A reboot is required for the changes to take effect.

## References:

1. NIST SP 800-53 Revision 5 :: SI-6 a

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230282  
Rule ID: SV-230282r854035  
STIG ID: RHEL-08-010450  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |

## 1.4 Configure Bootloader

The recommendations in this section focus on securing the bootloader and settings involved in the boot process directly.

### Notes:

- In Fedora 28 based distributions, the kernel command-line parameters for systems using the GRUB2 bootloader were defined in the `kernelopts` environment variable. This variable was stored in the `/boot/grub2/grubenv` file for each kernel boot entry. However, storing the kernel command-line parameters using `kernelopts` was not robust. Therefore, the `kernelopts` has been removed and the kernel command-line parameters are now stored in the Boot Loader Specification (BLS) snippet, instead of in the `/boot/loader/entries/<KERNEL_BOOT_ENTRY>.conf` file.
- Boot loader configuration files are unified across CPU architectures
  - Configuration files for the GRUB boot loader are now stored in the `/boot/grub2/` directory on all supported CPU architectures. The `/boot/efi/EFI/redhat/grub.cfg` file, which GRUB previously used as the main configuration file on UEFI systems, now simply loads the `/boot/grub2/grub.cfg` file.
  - This change simplifies the layout of the GRUB configuration file, improves user experience, and provides the following notable benefits:
    - You can boot the same installation with either EFI or legacy BIOS.
    - You can use the same documentation and commands for all architectures.
    - GRUB configuration tools are more robust, because they no longer rely on symbolic links and they do not have to handle platform-specific cases.
    - The usage of the GRUB configuration files is aligned with images generated by CoreOS Assembler (COSA) and OSBuild.
    - The usage of the GRUB configuration files is aligned with other Linux distributions.
    - Fedora 28 based distributions no longer boot on 32-bit UEFI
- Support for the 32-bit UEFI firmware was removed from the GRUB and shim boot loaders. As a consequence, Fedora 28 based distributions require a 64-bit UEFI, and can no longer boot on 64-bit systems that use a 32-bit UEFI.
  - The following packages have been removed as part of this change:
    - `grub2-efi-ia32`
    - `grub2-efi-ia32-cdboot`
    - `grub2-efi-ia32-modules`
    - `shim-ia32`

**Reference:** [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/8/html-single/considerations\\_in\\_adopting\\_rhel\\_8/index#kernel\\_considerations-in-adopting-RHEL-8](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html-single/considerations_in_adopting_rhel_8/index#kernel_considerations-in-adopting-RHEL-8)

## 1.4.1 Ensure bootloader password is set (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

### Description:

Setting the boot loader password will require that anyone rebooting the system must enter a password before being able to set command line boot parameters.

### Rationale:

Requiring a boot password upon execution of the boot loader will prevent an unauthorized user from entering boot parameters or changing the boot partition. This prevents users from weakening security (e.g. turning off SELinux at boot time).

### Impact:

If password protection is enabled, only the designated superuser can edit a GRUB 2 menu item by pressing **e** or access the GRUB 2 command line by pressing **c**

If GRUB 2 is set up to boot automatically to a password-protected menu entry the user has no option to back out of the password prompt to select another menu entry. Holding the SHIFT key will not display the menu in this case. The user must enter the correct username and password. If unable, the configuration files will have to be edited via the LiveCD or other means to fix the problem

### Audit:

Run the following script to verify the bootloader password has been set:

```
#!/usr/bin/env bash

{
  l_grub_password_file="$(find /boot -type f -name 'user.cfg' ! -empty)"
  if [ -f "$l_grub_password_file" ]; then
    awk -F. '/^\s*GRUB2_PASSWORD=\S+/ {print $1"."$2"."$3}'
    "$l_grub_password_file"
  fi
}
```

Output should be similar to:

```
GRUB2_PASSWORD=grub.pbkdf2.sha512
```

## Remediation:

Create an encrypted password with **grub2-setpassword**:

```
# grub2-setpassword  
  
Enter password: <password>  
Confirm password: <password>
```

## References:

1. NIST SP 800-53 Rev. 5: AC-3
2. NIST SP 800-53A :: AC-3.1

## Additional Information:

This recommendation is designed around the grub2 bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

**grub2-setpassword** outputs the **user.cfg** file which contains the hashed GRUB bootloader password. This utility only supports configurations where there is a single root user.

## Red Hat Enterprise Linux 8

```
Red Hat Enterprise Linux 8 STIG  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024  
  
GROUP ID: V-230234  
RULE ID: SV-230234r743922  
STIG ID: RHEL-08-010140  
SEVERITY: CAT I  
  
GROUP ID: V-230235  
RULE ID: SV-230235r743925  
STIG ID: RHEL-08-010150  
SEVERITY: CAT I
```



## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1542, T1542.000            | TA0003  | M1046       |

## *1.4.2 Ensure access to bootloader config is configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The grub files contain information on boot settings and passwords for unlocking boot options.

### **Rationale:**

Setting the permissions to read and write for root only prevents non-root users from seeing the boot parameters or changing them. Non-root users who read the boot parameters may be able to identify weaknesses in security upon boot and be able to exploit them.

### **Audit:**

Run the following script to verify grub configuration files:

- For systems using UEFI (Files located in `/boot/efi/EFI/*`):
  - Mode is `0700` or more restrictive
- For systems using BIOS (Files located in `/boot/grub2/*`):
  - Mode is `0600` or more restrictive
- Owner is the user `root`
- Group owner is group `root`

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    file_mug_chk()
    {
        l_out="" l_out2=""
        [[ "$(dirname "$l_file")" =~ ^\./boot\./efi\./EFI ]] && l_pmask="0077" ||
l_pmask="0177"
        l_maxperm="$( printf '%o' $(( 0777 & ~$l_pmask )) )"
        if [ $(( $l_mode & $l_pmask )) -gt 0 ]; then
            l_out2="$l_out2\n    - Is mode \"$l_mode\" and should be mode:
\"$l_maxperm\" or more restrictive"
        else
            l_out="$l_out\n    - Is correctly mode: \"$l_mode\" which is mode:
\"$l_maxperm\" or more restrictive"
        fi
        if [ "$l_user" = "root" ]; then
            l_out="$l_out\n    - Is correctly owned by user: \"$l_user\""
        else
            l_out2="$l_out2\n    - Is owned by user: \"$l_user\" and should be
owned by user: \"root\""
        fi
        if [ "$l_group" = "root" ]; then
            l_out="$l_out\n    - Is correctly group-owned by group: \"$l_user\""
        else
            l_out2="$l_out2\n    - Is group-owned by group: \"$l_user\" and
should be group-owned by group: \"root\""
        fi
        [ -n "$l_out" ] && l_output="$l_output\n    - File: \"$l_file\"$l_out\n"
        [ -n "$l_out2" ] && l_output2="$l_output2\n    - File:
\"$l_file\"$l_out2\n"
    }
    while IFS= read -r -d $'\0' l_gfile; do
        while read -r l_file l_mode l_user l_group; do
            file_mug_chk
            done <<< "$(stat -Lc '%n %a %U %G' "$l_gfile")"
            done <<(find /boot -type f \( -name 'grub*' -o -name 'user.cfg' \) -
print0)
            if [ -z "$l_output2" ]; then
                echo -e "\n- Audit Result:\n    *** PASS ***\n- * Correctly set *
:\n$l_output\n"
            else
                echo -e "\n- Audit Result:\n    ** FAIL **\n- * Reasons for audit
failure * :\n$l_output2\n"
                [ -n "$l_output" ] && echo -e " - * Correctly set * :\n$l_output\n"
            fi
        done
    done
}

```

## Remediation:

Run the following to update the mode, ownership, and group ownership of the grub configuration files:

- **IF** - the system uses UEFI (Files located in **/boot/efi/EFI/\***)

Edit **/etc/fstab** and add the **mask=0077**, **uid=0**, and **gid=0** options:

*Example:*

```
<device> /boot/efi vfat defaults,umask=0027,fmask=0077,uid=0,gid=0 0 0
```

**Note:** This may require a re-boot to enable the change

- **OR** -

- **IF** - the system uses BIOS (Files located in **/boot/grub2/\***)

Run the following commands to set ownership and permissions on your grub configuration file(s):

```
# [ -f /boot/grub2/grub.cfg ] && chown root:root /boot/grub2/grub.cfg
# [ -f /boot/grub2/grub.cfg ] && chmod u-x,go-rwx /boot/grub2/grub.cfg

# [ -f /boot/grub2/grubenv ] && chown root:root /boot/grub2/grubenv
# [ -f /boot/grub2/grubenv ] && chmod u-x,go-rwx /boot/grub2/grubenv

# [ -f /boot/grub2/user.cfg ] && chown root:root /boot/grub2/user.cfg
# [ -f /boot/grub2/user.cfg ] && chmod u-x,go-rwx /boot/grub2/user.cfg
```

## References:

1. NIST SP 800-53 Rev. 5: AC-3

## Additional Information:

This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 Protect Information through Access Control Lists</b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1542, T1542.000                   | TA0005, TA0007 | M1022              |

### 1.4.3 Ensure the operating system requires authentication for rescue mode (Automated)

#### Profile Applicability:

- STIG

#### Description:

Rescue mode provides the ability to boot a small Linux environment entirely from CD-ROM, or some other boot method, instead of the system's hard drive.

As the name implies, rescue mode is provided to rescue you from something. During normal operation, your Linux system uses files located on your system's hard drive to do everything — run programs, store your files, and more. However, there may be times when you are unable to get Linux running completely enough to access files on your system's hard drive. Using rescue mode, you can access the files stored on your system's hard drive, even if you cannot actually run Linux from that hard drive.

#### Rationale:

If the system does not require valid root authentication before it boots into emergency or rescue mode, anyone who invokes emergency or rescue mode is granted privileged access to all files on the system.

#### Audit:

Run the following command to verify the system requires authentication for rescue mode:

```
# grep -Psi -- '^h*ExecStart=-/usr/lib/systemd/systemd-sulogin-shell\h+rescue\b' /usr/lib/systemd/system/rescue.service
ExecStart=-/usr/lib/systemd/systemd-sulogin-shell rescue
```

#### Remediation:

Update `/usr/lib/systemd/system/rescue.service` and add or modify the following line:

```
ExecStart=-/usr/lib/systemd/systemd-sulogin-shell rescue
```

#### Default Value:

ExecStart=-/usr/lib/systemd/systemd-sulogin-shell rescue

#### References:

1. NIST SP 800-53 :: AC-3
2. NIST SP 800-53A :: AC-3.1

## Additional Information:

### Red Hat Enterprise Linux 8

Red Hat Enterprise Linux 8 STIG  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230236  
RULE ID: SV-230236r743928  
STIG ID: RHEL-08-010151  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques                                         | Tactics | Mitigations |
|---------------------------------------------------------------------|---------|-------------|
| T1078, T1078.001, T1078.002, T1078.003, T1078.004, T1110, T1110.004 | TA0006  | M1027       |

## *1.4.4 Ensure the operating system requires authentication upon booting into emergency mode (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system must require authentication upon booting into emergency mode.

### **Rationale:**

If the system does not require valid root authentication before it boots into emergency or rescue mode, anyone who invokes emergency or rescue mode is granted privileged access to all files on the system.

### **Audit:**

Check to see if the system requires authentication for emergency mode with the following command:

```
# grep sulogin-shell /usr/lib/systemd/system/emergency.service
ExecStart=-/usr/lib/systemd/systemd-sulogin-shell emergency
```

If the "ExecStart" line is configured for anything other than "/usr/lib/systemd/systemd-sulogin-shell emergency", commented out, or missing, this is a finding.

### **Remediation:**

Configure the system to require authentication upon booting into emergency mode by adding the following line to the "/usr/lib/systemd/system/emergency.service" file.

```
ExecStart=-/usr/lib/systemd/systemd-sulogin-shell emergency
```

### **References:**

1. NIST SP 800-53 :: AC-3
2. NIST SP 800-53A :: AC-3.1



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244523  
Rule ID: SV-244523r743818  
STIG ID: RHEL-08-010152  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

### 1.4.5 Ensure a unique name is set as the superusers account (BIOS) (Automated)

#### Profile Applicability:

- STIG

#### Description:

Operating systems booted with a BIOS must require a unique superusers name upon booting into single-user and maintenance modes.

#### Rationale:

If the system does not require valid authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 8 operating systems and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

#### Audit:

For systems that use UEFI, this is Not Applicable.  
Verify that a unique name is set as the "superusers" account:

```
# grep -iw "superusers" /boot/grub2/grub.cfg  
  
set superusers="[someuniquestringhere]"  
  
export superusers
```

If "superusers" is not set to a unique name or is missing a name, this is a finding.

#### Remediation:

Configure the system to have a unique name for the grub superusers account.  
Edit the /etc/grub.d/01\_users file and add or modify the following lines:

```
set superusers="[someuniquestringhere]"  
export superusers  
password_pbkdf2 [someuniquestringhere] ${GRUB2_PASSWORD}
```

Generate a new grub.cfg file with the following command:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

#### References:

1. NIST SP 800-53 :: AC-3
2. NIST SP 800-53A :: AC-3.1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244522  
Rule ID: SV-244522r792984  
STIG ID: RHEL-08-010149  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

## 1.4.6 Ensure a unique name is set as the superusers account (UEFI) (Automated)

### Profile Applicability:

- STIG

### Description:

Operating systems booted with United Extensible Firmware Interface (UEFI) must require a unique superusers name upon booting into single-user mode and maintenance.

### Rationale:

If the system does not require valid authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for RHEL 8 operating systems and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

### Audit:

For systems that use BIOS, this is Not Applicable.

Verify that a unique name is set as the "superusers" account:

```
# grep -iw "superusers" /boot/efi/EFI/redhat/grub.cfg

set superusers="[someuniquestringhere]"

export superusers
```

If "superusers" is not set to a unique name or is missing a name, this is a finding.

### Remediation:

Configure the system to have a unique name for the grub superusers account.

Edit the /etc/grub.d/01\_users file and add or modify the following lines:

```
set superusers="[someuniquestringhere]"
export superusers
password_pbkdf2 [someuniquestringhere] ${GRUB2_PASSWORD}
```

Generate a new grub.cfg file with the following command:

```
# grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
```

### References:

1. NIST SP 800-53 :: AC-3
2. NIST SP 800-53A :: AC-3.1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244521  
Rule ID: SV-244521r792982  
STIG ID: RHEL-08-010141  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

### *1.4.7 Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed seven times within two seconds (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The systemd Ctrl-Alt-Delete burst key sequence must be disabled.

#### **Rationale:**

A locally logged-on user who presses Ctrl-Alt-Delete when at the console can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot. In a graphical user environment, risk of unintentional reboot from the Ctrl-Alt-Delete sequence is reduced because the user will be prompted before any action is taken.

#### **Audit:**

Verify the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed seven times within two seconds with the following command:

```
# grep -i ctrl /etc/systemd/system.conf  
CtrlAltDelBurstAction=none
```

If the "CtrlAltDelBurstAction" is not set to "none", commented out, or is missing, this is a finding.

#### **Remediation:**

Configure the system to disable the CtrlAltDelBurstAction by added or modifying the following line in the "/etc/systemd/system.conf" configuration file:

```
CtrlAltDelBurstAction=none
```

Reload the daemon for this change to take effect.

```
# systemctl daemon-reload
```

#### **References:**

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230531  
Rule ID: SV-230531r627750  
STIG ID: RHEL-08-040172  
Severity: CAT I

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

## 1.4.8 Ensure GRUB 2 is configured to enable page poisoning to mitigate use-after-free vulnerabilities (Automated)

### Profile Applicability:

- STIG

### Description:

The operating system must clear the page allocator to prevent use-after-free attacks.

### Rationale:

Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can be either hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

Poisoning writes an arbitrary value to freed pages, so any modification or reference to that page after being freed or before being initialized will be detected and prevented. This prevents many types of use-after-free vulnerabilities at little performance cost. Also prevents leak of data and detection of corrupted memory.

Satisfies: SRG-OS-000134-GPOS-00068, SRG-OS-000433-GPOS-00192

### Audit:

Verify that GRUB 2 is configured to enable page poisoning to mitigate use-after-free vulnerabilities with the following commands:

Check that the current GRUB 2 configuration has page poisoning enabled:

```
# grub2-editenv list | grep page_poison

kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto
resume=/dev/mapper/rhel-swap rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb
quiet fips=1 page_poison=1 vsyscall=none audit=1 audit_backlog_limit=8192
boot=UUID=8d171156-cd61-421c-ba41-1c021ac29e82
```

If "page\_poison" is not set to "1" or is missing, this is a finding.

Check that page poisoning is enabled by default to persist in kernel updates:

```
# grep page_poison /etc/default/grub

GRUB_CMDLINE_LINUX="page_poison=1"
```

If "page\_poison" is not set to "1", is missing or commented out, this is a finding.



## Remediation:

Configure the operating system to enable page poisoning with the following commands:

```
# grubby --update-kernel=ALL --args="page_poison=1"
```

Add or modify the following line in "/etc/default/grub" to ensure the configuration survives kernel updates:

```
GRUB_CMDLINE_LINUX="page_poison=1"
```

## References:

1. NIST SP 800-53 :: SC-3
2. NIST SP 800-53A :: SC-3.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230277  
Rule ID: SV-230277r792884  
STIG ID: RHEL-08-010421  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### *1.4.9 Ensure GRUB 2 is configured to enable poisoning of SLUB/SLAB objects to mitigate use-after-free vulnerabilities (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must clear SLUB/SLAB objects to prevent use-after-free attacks.

#### **Rationale:**

Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can be either hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

Poisoning writes an arbitrary value to freed pages, so any modification or reference to that page after being freed or before being initialized will be detected and prevented. This prevents many types of use-after-free vulnerabilities at little performance cost. Also prevents leak of data and detection of corrupted memory.

SLAB objects are blocks of physically-contiguous memory. SLUB is the unqueued SLAB allocator.

Satisfies: SRG-OS-000134-GPOS-00068, SRG-OS-000433-GPOS-00192

## Audit:

Verify that GRUB 2 is configured to enable poisoning of SLUB/SLAB objects to mitigate use-after-free vulnerabilities with the following commands:

Check that the current GRUB 2 configuration has poisoning of SLUB/SLAB objects enabled:

```
# grub2-editenv - list | grep slub_debug

kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto
resume=/dev/mapper/rhel-swap rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb
quiet fips=1 slub_debug=P page_poison=1 vsyscall=none audit=1
audit_backlog_limit=8192 boot=UUID=8d171156-cd61-421c-ba41-1c021ac29e82
```

If "slub\_debug" is not set to "P" or is missing, this is a finding.

Check that poisoning of SLUB/SLAB objects is enabled by default to persist in kernel updates:

```
# grep slub_debug /etc/default/grub

GRUB_CMDLINE_LINUX="slub_debug=P"
```

If "slub\_debug" is not set to "P", is missing or commented out, this is a finding.

## Remediation:

Configure the operating system to enable poisoning of SLUB/SLAB objects with the following commands:

```
# grubby --update-kernel=ALL --args="slub_debug=P"
```

Add or modify the following line in "/etc/default/grub" to ensure the configuration survives kernel updates:

```
GRUB_CMDLINE_LINUX="slub_debug=P"
```

## References:

1. NIST SP 800-53A :: SC-3.1 (ii)

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230279  
Rule ID: SV-230279r951598  
STIG ID: RHEL-08-010423  
Severity: CAT II

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

## 1.4.10 Ensure GRUB 2 is configured to disable vsyscalls (Automated)

### Profile Applicability:

- STIG

### Description:

The operating system must disable virtual syscalls.

### Rationale:

Syscalls are special routines in the Linux kernel, which userspace applications ask to do privileged tasks. Invoking a system call is an expensive operation because the processor must interrupt the currently executing task and switch context to kernel mode and then back to userspace after the system call completes. Virtual syscalls map into user space a page that contains some variables and the implementation of some system calls. This allows the system calls to be executed in userspace to alleviate the context switching expense.

Virtual syscalls provide an opportunity of attack for a user who has control of the return instruction pointer. Disabling vsyscalls help to prevent return oriented programming (ROP) attacks via buffer overflows and overruns. If the system intends to run containers based on RHEL 6 components, then virtual syscalls will need to be enabled so the components function properly.

Satisfies: SRG-OS-000134-GPOS-00068, SRG-OS-000433-GPOS-00192

### Audit:

Verify that GRUB 2 is configured to disable vsyscalls with the following commands:  
Check that the current GRUB 2 configuration disables vsyscalls:

```
# grub2-editenv list | grep vsyscall

kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto
resume=/dev/mapper/rhel-swap rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb
quiet fips=1 page_poison=1 vsyscall=none audit=1 audit_backlog_limit=8192
boot=UUID=8d171156-cd61-421c-ba41-1c021ac29e82
```

If "vsyscall" is not set to "none" or is missing, this is a finding.

Check that vsyscalls are disabled by default to persist in kernel updates:

```
# grep vsyscall /etc/default/grub

GRUB_CMDLINE_LINUX="vsyscall=none"
```

If "vsyscall" is not set to "none", is missing or commented out and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

## Remediation:

Document the use of vsyscalls with the ISSO as an operational requirement or disable them with the following command:

```
# grubby --update-kernel=ALL --args="vsyscall=none"
```

Add or modify the following line in "/etc/default/grub" to ensure the configuration survives kernel updates:

```
GRUB_CMDLINE_LINUX="vsyscall=none"
```

## References:

1. NIST SP 800-53 Revision 5 :: SC-3
2. NIST SP 800-53A :: SC-3.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230278  
Rule ID: SV-230278r792886  
STIG ID: RHEL-08-010422  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

## 1.5 Configure Additional Process Hardening

### *1.5.1 Ensure address space layout randomization is enabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### **Description:**

Address space layout randomization (ASLR) is an exploit mitigation technique which randomly arranges the address space of key data areas of a process.

#### **Rationale:**

Randomly placing virtual memory regions will make it difficult to write memory page exploits as the memory placement will be consistently shifting.

#### **Audit:**

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `kernel.randomize_va_space` is set to 2

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.



```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); a_parlist=(kernel.randomize_va_space=2)
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F= '{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\"")
            "      in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"") \
            "      in the running configuration" \
            "      and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="$l_out// # /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_file")
                fi
            fi
            done < <("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([\^#\n\r]+|\#\h*\[/[\^#\n\r\h]+\.\conf\b)')
            if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
                l_kpar="$(grep -Po "^\h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
                l_kpar="$l_kpar//\./."
                [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_ufwscf")
            fi
            if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
                while IFS="" read -r l_fkpname l_file_parameter_value; do
                    l_fkpname="$l_fkpname// /}";
l_file_parameter_value="$l_file_parameter_value// /}"
                    if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_file_parameter_value"; then
                        a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\"") \
                        "      in \"$(printf '%s' "${A_out[@]}")\"")
                    else
                        a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\"") \
                        "      in \"$(printf '%s' "${A_out[@]}")\"") \
                        "      and should have a value of: \"$l_value_out\"")
                    fi
                done
            fi
        }
    }
}

```

```

done < <(grep -Po -- "\h*$l_parameter_name\h*=\h*\H+"
"${A_out[@]}")
else
a_output2+=(" - \"$l_parameter_name\" is not set in an included
file" \
    ** Note: \"$l_parameter_name\" May be set in a file that's
ignored by load procedure **)
fi
}
l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
while IFS="=" read -r l_parameter_name l_parameter_value; do # Assess and
check parameters
l_parameter_name="${l_parameter_name// /}";
l_parameter_value="${l_parameter_value// /}"
l_value_out="${l_parameter_value//-/ through }";
l_value_out="${l_value_out//|/ or }"
l_value_out="$(tr -d '(){}' <<< "$l_value_out")"
f_kernel_parameter_chk
done < <(printf '%s\n' "${a_parlist[@]}")
if [ "${#a_output2[@]}" -le 0 ]; then
printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
else
printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
[ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:"
"${a_output[@]}" ""
fi
}

```

## Remediation:

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `kernel.randomize_va_space = 2`

### Example:

```

# printf "
kernel.randomize_va_space = 2
" >> /etc/sysctl.d/60-kernel_sysctl.conf

```

Run the following command to set the active kernel parameter:

```

# sysctl -w kernel.randomize_va_space=2

```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## Default Value:

`kernel.randomize_va_space = 2`

## References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 Rev. 5: CM-6
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 5 :: SI-16

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230280  
Rule ID: SV-230280r858767  
STIG ID: RHEL-08-010430  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>10.5 <u>Enable Anti-Exploitation Features</u></b><br>Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.                                                                                                  |      | ●    | ●    |
| v7               | <b>8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u></b><br>Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables. |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1068, T1068.000            | TA0002  | M1050       |

## 1.5.2 Ensure ptrace\_scope is restricted (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The `ptrace()` system call provides a means by which one process (the "tracer") may observe and control the execution of another process (the "tracee"), and examine and change the tracee's memory and registers.

The `sysctl` settings (writable only with `CAP_SYS_PTRACE`) are:

- **0** - classic ptrace permissions: a process can `PTRACE_ATTACH` to any other process running under the same uid, as long as it is dumpable (i.e. did not transition uids, start privileged, or have called `prctl(PR_SET_DUMPABLE...)` already). Similarly, `PTRACE_TRACEME` is unchanged.
- **1** - restricted ptrace: a process must have a predefined relationship with the inferior it wants to call `PTRACE_ATTACH` on. By default, this relationship is that of only its descendants when the above classic criteria is also met. To change the relationship, an inferior can call `prctl(PR_SET_PTRACER, debugger, ...)` to declare an allowed debugger PID to call `PTRACE_ATTACH` on the inferior. Using `PTRACE_TRACEME` is unchanged.
- **2** - admin-only attach: only processes with `CAP_SYS_PTRACE` may use ptrace with `PTRACE_ATTACH`, or through children calling `PTRACE_TRACEME`.
- **3** - no attach: no processes may use ptrace with `PTRACE_ATTACH` nor via `PTRACE_TRACEME`. Once set, this `sysctl` value cannot be changed.

### Rationale:

If one application is compromised, it would be possible for an attacker to attach to other running processes (e.g. Bash, Firefox, SSH sessions, GPG agent, etc) to extract additional credentials and continue to expand the scope of their attack.

Enabling restricted mode will limit the ability of a compromised process to `PTRACE_ATTACH` on other processes running under the same user. With restricted mode, ptrace will continue to work with root user.

**Audit:**

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `kernel.yama.ptrace_scope` is set to a value of: 1, 2, or 3

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); a_parlist=("kernel.yama.pttrace_scope=(1|2|3)")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F= '{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\""
                "    in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"" \
                "    in the running configuration" \
                "    and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="$l_out// # /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_file")
                fi
            fi
            done < <("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([\^#\n\r]+|\#\h*\[/[\^#\n\r\h]+\.\conf\b)')
            if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
                l_kpar="$(grep -Po "^\h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
                l_kpar="$l_kpar//\./."
                [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_ufwscf")
            fi
            if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
                while IFS="" read -r l_fkpname l_file_parameter_value; do
                    l_fkpname="$l_fkpname// /}";
l_file_parameter_value="$l_file_parameter_value// /}"
                    if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_file_parameter_value"; then
                        a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\"" \
                            "    in \"$(printf '%s' "${A_out[@]}")\"")
                    else
                        a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\""
                            "    in \"$(printf '%s' "${A_out[@]}")\"" \
                            "    and should have a value of: \"$l_value_out\"")
                    fi
                done
            fi
        }
    }
}

```

```

done < <(grep -Po -- "\^h*$l_parameter_name\h*=\h*\H+"
"${A_out[@]}")
else
a_output2+=(" - \"$l_parameter_name\" is not set in an included
file" \
    ** Note: \"$l_parameter_name\" May be set in a file that's
ignored by load procedure **)
fi
}
l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
while IFS="=" read -r l_parameter_name l_parameter_value; do # Assess and
check parameters
l_parameter_name="${l_parameter_name// /}";
l_parameter_value="${l_parameter_value// /}"
l_value_out="${l_parameter_value//-/ through }";
l_value_out="${l_value_out//|/ or }"
l_value_out="$(tr -d '()' <<< "$l_value_out")"
f_kernel_parameter_chk
done < <(printf '%s\n' "${a_parlist[@]}")
if [ "${#a_output2[@]}" -le 0 ]; then
printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
else
printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
[ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:"
"${a_output[@]}" ""
fi
}

```

## Remediation:

Set the **kernel.yama.ptrace\_scope** parameter in **/etc/sysctl.conf** or a file in **/etc/sysctl.d/** ending in **.conf** to a value of **1, 2, or 3**:

```

kernel.yama.ptrace_scope = 1
- OR -
kernel.yama.ptrace_scope = 2
- OR -
kernel.yama.ptrace_scope = 3

```

### Example:

```

# printf "%s\n" "kernel.yama.ptrace_scope = 1" >> /etc/sysctl.d/60-
kernel_sysctl.conf

```

Run the following command to set the active kernel parameter:

```

# sysctl -w kernel.yama.ptrace_scope=1

```

## Note:

- If a value of **2** or **3** is preferred, or required by local site policy, replace the **1** with the desired value of **2** or **3** in the example above
- If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten

### Default Value:

kernel.yama.ptrace\_scope = 0

### References:

1. <https://www.kernel.org/doc/Documentation/security/Yama.txt>
2. <https://github.com/raj3shp/termspy>
3. NIST SP 800-53 Rev. 5: CM-6

### Additional Information:

Ptrace is very rarely used by regular applications and is mostly used by debuggers such as **gdb** and **strace**.

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |    |    |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1055, T1055.008            | TA0005  | M1040       |



### *1.5.3 Ensure core dump backtraces are disabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

A core dump is the memory of an executable program. It is generally used to determine why a program aborted. It can also be used to glean confidential information from a core file.

#### **Rationale:**

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems, increasing the risk to the system.

#### **Audit:**

Run the following script to verify `ProcessSizeMax` is set to `0` in `/etc/systemd/coredump.conf` or a file in the `/etc/systemd/coredump.conf.d/` directory:

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); a_parlist=("ProcessSizeMax=0")
    l_systemd_config_file="/etc/systemd/coredump.conf" # Main systemd
configuration file
    f_config_file_parameter_chk()
    {
        unset A_out; declare -A A_out # Check config file(s) setting
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//# /}"
                else
                    l_systemd_parameter="$(awk -F= '{print $1}' <<< "$l_out" |
xargs) "
                    grep -Piq -- "\h*$l_systemd_parameter_name\b" <<<
"$l_systemd_parameter" && A_out+=(["$l_systemd_parameter"]="$l_file")
                fi
            fi
            done < <("$l_systemdanalyze" cat-config "$l_systemd_config_file" | grep
-Pio '\h*([\#\n\r]+|\#\h*\/[\#\n\r\h]+\.conf\b)')
            if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
                while IFS="" read -r l_systemd_file_parameter_name
l_systemd_file_parameter_value; do
                    l_systemd_file_parameter_name="${l_systemd_file_parameter_name//
/}"
l_systemd_file_parameter_value="${l_systemd_file_parameter_value// /}"
                    if grep -Piq "\b$l_systemd_parameter_value\b" <<<
"$l_systemd_file_parameter_value"; then
                        a_output+=(" - \"$l_systemd_parameter_name\" is correctly set
to \"$l_systemd_file_parameter_value\" \" \" \
                        " in \"$(printf '%s' "${A_out[@]}")\"")
                    else
                        a_output2+=(" - \"$l_systemd_parameter_name\" is incorrectly
set to \"$l_systemd_file_parameter_value\" \" \" \
                        " in \"$(printf '%s' "${A_out[@]}")\" and should have a
value matching: \"$l_value_out\"")
                    fi
                done < <(grep -Pio -- "\h*$l_systemd_parameter_name\h*=\h*\H+"
"${A_out[@]}")
                else
                    a_output2+=(" - \"$l_systemd_parameter_name\" is not set in an
included file" \
                    " *** Note: \"$l_systemd_parameter_name\" May be set in a file
that's ignored by load procedure ***")
                fi
            }
            l_systemdanalyze="$(readlink -f /bin/systemd-analyze)"
            while IFS="" read -r l_systemd_parameter_name l_systemd_parameter_value;
do # Assess and check parameters
                l_systemd_parameter_name="${l_systemd_parameter_name// /}";
l_systemd_parameter_value="${l_systemd_parameter_value// /}"
                l_value_out="${l_systemd_parameter_value//-/ through }";
l_value_out="${l_value_out//|/ or }"

```

```

l_value_out="$(tr -d '()' <<< "$l_value_out")"
f_config_file_parameter_chk
done < <(printf '%s\n' "${a_parlist[@]}")
if [ "${#a_output2[@]}" -le 0 ]; then
    printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
else
    printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
    [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:"
"${a_output[@]}" ""
fi
}

```

## Remediation:

Create or edit the file `/etc/systemd/coredump.conf`, or a file in the `/etc/systemd/coredump.conf.d` directory ending in `.conf`.

Edit or add the following line in the `[Coredump]` section:

```
ProcessSizeMax=0
```

## Example:

```

#!/usr/bin/env bash

{
    [ ! -d /etc/systemd/coredump.conf.d/ ] && mkdir
/etc/systemd/coredump.conf.d/
    if grep -Psq -- '^h*[Coredump\]' /etc/systemd/coredump.conf.d/60-
coredump.conf; then
        printf '%s\n' "ProcessSizeMax=0" >> /etc/systemd/coredump.conf.d/60-
coredump.conf
    else
        printf '%s\n' "[Coredump]" "ProcessSizeMax=0" >>
/etc/systemd/coredump.conf.d/60-coredump.conf
    fi
}

```

## Default Value:

ProcessSizeMax=2G

## References:

1. <https://www.freedesktop.org/software/systemd/man/coredump.conf.html>
2. NIST SP 800-53 Rev. 5: CM-6b
3. NIST SP 800-53A :: CM-6.1 (iv)

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230315  
Rule ID: SV-230315r627750  
STIG ID: RHEL-08-010675  
Severity: CAT II

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1005, T1005.000            | TA0007  | M1057       |

## *1.5.4 Ensure core dump storage is disabled (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

A core dump is the memory of an executable program. It is generally used to determine why a program aborted. It can also be used to glean confidential information from a core file.

### **Rationale:**

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems.

### **Audit:**

Run the following script to verify **Storage** is set to **none** in **/etc/systemd/coredump.conf** or a file in the **/etc/systemd/coredump.conf.d/** directory:

```
#!/usr/bin/env bash

{
    a_output=(); a_output2=(); a_parlist=("Storage=none")
    l_systemd_config_file="/etc/systemd/coredump.conf" # Main systemd
configuration file
    f_config_file_parameter_chk()
    {
        unset A_out; declare -A A_out # Check config file(s) setting
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="$l_out// # /}"
                else
                    l_systemd_parameter="$ (awk -F= '{print $1}' <<< "$l_out" |
xargs)"
                    grep -Piq -- "^\h*$l_systemd_parameter_name\b" <<<
"$l_systemd_parameter" && A_out+=(["$l_systemd_parameter"]="$l_file")
                    fi
                done << ("$l_systemd_analyze" cat-config "$l_systemd_config_file" | grep
-Pio '^\h*([\#\n\r]+|\#\h*\[/[\#\n\r\h]+\conf\b)')
                if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
                    while IFS="=" read -r l_systemd_file_parameter_name
l_systemd_file_parameter_value; do
                        l_systemd_file_parameter_name="$ {l_systemd_file_parameter_name//
/}"
                        l_systemd_file_parameter_value="$ {l_systemd_file_parameter_value// /}"
                        if grep -Piq "\b$l_systemd_parameter_value\b" <<<
"$l_systemd_file_parameter_value"; then
                            a_output+=(" - \"$l_systemd_parameter_name\" is correctly set
to \"$l_systemd_file_parameter_value\" \" \"
                                \" in \"$(printf '%s' "${A_out[@]}")\" \" \" )
                        else
                            a_output2+=(" - \"$l_systemd_parameter_name\" is incorrectly
set to \"$l_systemd_file_parameter_value\" \" \" \"
                                \" in \"$(printf '%s' "${A_out[@]}")\" \" and should have a
value matching: \"$l_value_out\" \" \" )
                        fi
                    done << (grep -Pio -- "^\h*$l_systemd_parameter_name\h*=\h*\H+"
"${A_out[@]}")
                    else
                        a_output2+=(" - \"$l_systemd_parameter_name\" is not set in an
included file \" \"
                            \" *** Note: \"$l_systemd_parameter_name\" May be set in a file
that's ignored by load procedure *** \" \" )
                    fi
                }
                l_systemd_analyze="$ (readlink -f /bin/systemd-analyze)"
                while IFS="=" read -r l_systemd_parameter_name l_systemd_parameter_value;
do # Assess and check parameters
                    l_systemd_parameter_name="$ {l_systemd_parameter_name// /}";
                    l_systemd_parameter_value="$ {l_systemd_parameter_value// /}"
                    l_value_out="$ {l_systemd_parameter_value// - / through }";
                    l_value_out="$ {l_value_out// / or }"

```

```

l_value_out="$(tr -d '()' <<< "$l_value_out")"
f_config_file_parameter_chk
done < <(printf '%s\n' "${a_parlist[@]}")
if [ "${#a_output2[@]}" -le 0 ]; then
    printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
else
    printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
    [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:"
"${a_output[@]}" ""
fi
}

```

## Remediation:

Create or edit the file `/etc/systemd/coredump.conf`, or a file in the `/etc/systemd/coredump.conf.d` directory ending in `.conf`.

Edit or add the following line in the `[Coredump]` section:

```
Storage=none
```

## Example:

```

#!/usr/bin/env bash

{
    [ ! -d /etc/systemd/coredump.conf.d/ ] && mkdir
/etc/systemd/coredump.conf.d/
    if grep -Psq -- '^h*\[Coredump\]' /etc/systemd/coredump.conf.d/60-
coredump.conf; then
        printf '%s\n' "Storage=none" >> /etc/systemd/coredump.conf.d/60-
coredump.conf
    else
        printf '%s\n' "[Coredump]" "Storage=none" >>
/etc/systemd/coredump.conf.d/60-coredump.conf
    fi
}

```

## References:

1. <https://www.freedesktop.org/software/systemd/man/coredump.conf.html>
2. NIST SP 800-53 Revision 5 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230314  
Rule ID: SV-230314r627750  
STIG ID: RHEL-08-010674  
Severity: CAT II

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1005, T1005.000            | TA0007  | M1057       |



### 1.5.5 Ensure the storing of core dumps is disabled (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must disable the kernel.core\_pattern.

#### Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

#### Audit:

Verify the operating system disables storing core dumps with the following commands:

```
# sysctl kernel.core_pattern  
kernel.core_pattern = |/bin/false
```

If the returned line does not have a value of "|/bin/false", or a line is not returned and the need for core dumps is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Verify the configuration files are present to enable this kernel parameter:

```
# grep -r kernel.core_pattern /run/sysctl.d/*.conf  
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf  
/etc/sysctl.conf /etc/sysctl.d/*.conf  
  
/etc/sysctl.d/99-sysctl.conf:kernel.core_pattern = |/bin/false
```

If "kernel.core\_pattern" is not set to "|/bin/false", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

## Remediation:

Configure the operating system to disable the storing core dumps by adding the following line to a file in the "/etc/sysctl.d" directory:

```
kernel.core_pattern = |/bin/false
```

Remove any configurations that conflict with the above from the following locations:

*/run/sysctl.d/.conf*

*/usr/local/lib/sysctl.d/.conf*

*/usr/lib/sysctl.d/.conf*

*/lib/sysctl.d/.conf*

*/etc/sysctl.conf*

*/etc/sysctl.d/\*.conf*

The system configuration files need to be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
# sysctl --system
```

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230311

Rule ID: SV-230311r858769

STIG ID: RHEL-08-010671

Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

## 1.5.6 Ensure the operating system is not configured to acquire save or process core dumps (Automated)

### Profile Applicability:

- STIG

### Description:

The operating system must disable acquiring, saving, and processing core dumps.

### Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems.

When the kernel invokes systemd-coredump to handle a core dump, it runs in privileged mode, and will connect to the socket created by the systemd-coredump.socket unit. This, in turn, will spawn an unprivileged systemd-coredump@.service instance to process the core dump.

### Audit:

Verify the operating system is not configured to acquire, save, or process core dumps with the following command:

```
# systemctl status systemd-coredump.socket

systemd-coredump.socket
Loaded: masked (Reason: Unit ctrl-alt-del.target is masked.)
Active: inactive (dead)
```

If "systemd-coredump.socket" is loaded and not masked and the need for core dumps is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

## Remediation:

Configure the system to disable "systemd-coredump.socket" with the following command:

```
# systemctl disable --now systemd-coredump.socket
# systemctl mask systemd-coredump.socket

Created symlink /etc/systemd/system/systemd-coredump.socket -> /dev/null
```

Reload the daemon for this change to take effect.

```
# systemctl daemon-reload
```

## References:

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230312  
Rule ID: SV-230312r833308  
STIG ID: RHEL-08-010672  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

## 1.5.7 Ensure kernel core dumps are disabled unless needed (Automated)

### Profile Applicability:

- STIG

### Description:

The operating system must disable kernel dumps unless needed.

### Rationale:

Kernel core dumps may contain the full contents of system memory at the time of the crash. Kernel core dumps may consume a considerable amount of disk space and may result in denial of service by exhausting the available space on the target file system partition.

The operating system's installation media presents the option to enable or disable the "kdump" service at the time of system installation.

### Audit:

Verify that kernel core dumps are disabled unless needed with the following command:

```
# sudo systemctl status kdump.service

kdump.service - Crash recovery kernel arming
Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled; vendor
preset: enabled)
Active: active (exited) since Mon 2020-05-04 16:08:09 EDT; 3min ago
Main PID: 1130 (code=exited, status=0/SUCCESS)
```

If the "kdump" service is active, ask the System Administrator if the use of the service is required and documented with the Information System Security Officer (ISSO).  
If the service is active and is not documented, this is a finding.

### Remediation:

If kernel core dumps are not required, disable the "kdump" service with the following command:

```
# systemctl disable kdump.service
```

If kernel core dumps are required, document the need with the ISSO.

### References:

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230310  
Rule ID: SV-230310r627750  
STIG ID: RHEL-08-010670  
Severity: CAT II

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### *1.5.8 Ensure the operating system enables hardening for the BPF JIT (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must enable hardening for the Berkeley Packet Filter Just-in-time compiler.

#### **Rationale:**

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Enabling hardening for the Berkeley Packet Filter (BPF) Just-in-time (JIT) compiler aids in mitigating JIT spraying attacks. Setting the value to "2" enables JIT hardening for all users.

#### **Audit:**

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.core.bpf_jit_harden` is set to 2

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); a_parlist=(net.core.bpf_jit_harden=2)
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F= '{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\"")
            "    in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"") \
            "    in the running configuration" \
            "    and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="$l_out// # /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_file")
                fi
            fi
            done < <("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([\^#\n\r]+|\#\h*\[/[\^#\n\r\h]+\.\conf\b)')
            if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
                l_kpar="$(grep -Po "^\h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
                l_kpar="$l_kpar//\./}"
                [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_ufwscf")
            fi
            if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
                while IFS="" read -r l_fkpname l_file_parameter_value; do
                    l_fkpname="$l_fkpname// /}";
                    l_file_parameter_value="$l_file_parameter_value// /}"
                    if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_file_parameter_value"; then
                        a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\"") \
                        "    in \"$(printf '%s' "${A_out[@]}")\"")
                    else
                        a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\"") \
                        "    in \"$(printf '%s' "${A_out[@]}")\"") \
                        "    and should have a value of: \"$l_value_out\"")
                    fi
                done
            fi
        }
    }
}

```



```

done < <(grep -Po -- "\h*$l_parameter_name\h*=\h*\H+"
"${A_out[@]}")
else
a_output2+=(" - \"$l_parameter_name\" is not set in an included
file" \
    ** Note: \"$l_parameter_name\" May be set in a file that's
ignored by load procedure **)
fi
}
l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
while IFS="=" read -r l_parameter_name l_parameter_value; do # Assess and
check parameters
l_parameter_name="${l_parameter_name// /}";
l_parameter_value="${l_parameter_value// /}"
l_value_out="${l_parameter_value//-/ through }";
l_value_out="${l_value_out//|/ or }"
l_value_out="$(tr -d '()' <<< "$l_value_out")"
f_kernel_parameter_chk
done < <(printf '%s\n' "${a_parlist[@]}")
if [ "${#a_output2[@]}" -le 0 ]; then
printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
else
printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
[ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:"
"${a_output[@]}" ""
fi
}

```

## Remediation:

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.core.bpf_jit_harden = 2`

### Example:

```
# printf "%s\n" "net.core.bpf_jit_harden = 2" >> /etc/sysctl.d/60-
net_core_sysctl.conf
```

Run the following command to set the active kernel parameter:

```
# sysctl -w net.core.bpf_jit_harden=2
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## Default Value:

`net.core.bpf_jit_harden = 1`

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244554  
Rule ID: SV-244554r858832  
STIG ID: RHEL-08-040286  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

### *1.5.9 Ensure kernel page-table isolation is enabled (Automated)*

**Profile Applicability:**

- STIG

**Description:**

The operating system must enable mitigations against processor-based vulnerabilities.

**Rationale:**

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, games, software packages, tools, and demonstration software not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

Verify the operating system is configured to disable non-essential capabilities. The most secure way of ensuring a non-essential capability is disabled is to not have the capability installed.

Kernel page-table isolation is a kernel feature that mitigates the Meltdown security vulnerability and hardens the kernel against attempts to bypass kernel address space layout randomization (KASLR).

## Audit:

Verify the operating system enables kernel page-table isolation with the following commands:

```
# grub2-editenv - list | grep pti

kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto
resume=/dev/mapper/rhel-swap rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb
quiet fips=1 audit=1 audit_backlog_limit=8192 pti=on boot=UUID=8d171156-cd61-421c-ba41-1c021ac29e82
```

If the "pti" entry does not equal "on", is missing, or the line is commented out, this is a finding.

Check that kernel page-table isolation is enabled by default to persist in kernel updates:

```
# grep audit /etc/default/grub

GRUB_CMDLINE_LINUX="pti=on"
```

If "pti" is not set to "on", is missing or commented out, this is a finding.

## Remediation:

Configure the operating system to enable kernel page-table isolation with the following command:

```
# grubby --update-kernel=ALL --args="pti=on"
```

Add or modify the following line in "/etc/default/grub" to ensure the configuration survives kernel updates:

```
GRUB_CMDLINE_LINUX="pti=on"
```

## References:

1. NIST SP 800-53 Revision 5 :: CM-7 a
2. NIST SP 800-53A :: CM-7.1 (ii)

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230491  
Rule ID: SV-230491r818842  
STIG ID: RHEL-08-040004  
Severity: CAT III

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### 1.5.10 Ensure the NX (no-execution) bit flag is set on the system (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must implement non-executable data to protect its memory from unauthorized code execution.

#### Rationale:

Some adversaries launch attacks with the intent of executing code in non-executable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can be either hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

Examples of attacks are buffer overflow attacks.

#### Audit:

Verify the NX (no-execution) bit flag is set on the system.

Check that the no-execution bit flag is set with the following commands:

```
# dmesg | grep NX  
[ 0.000000] NX (Execute Disable) protection: active
```

If "dmesg" does not show "NX (Execute Disable) protection" active, check the cpuinfo settings with the following command:

```
# less /proc/cpuinfo | grep -i flags  
flags : fpu vme de pse tsc ms nx rdtscp lm constant_tsc
```

If "flags" does not contain the "nx" flag, this is a finding.

#### Remediation:

The NX bit execute protection must be enabled in the system BIOS.

#### References:

1. NIST SP 800-53 Revision 5 :: SI-16

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230276  
Rule ID: SV-230276r854031  
STIG ID: RHEL-08-010420  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>10.5 <u>Enable Anti-Exploitation Features</u></b><br>Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.                                                                                                  |      |  |  |
| v7               | <b>8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u></b><br>Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables. |      |  |  |

### *1.5.11 Ensure the operating system disables the use of user namespaces (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must disable the use of user namespaces.

The `sysctl --system` command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored.

`/etc/sysctl.d/.conf /run/sysctl.d/.conf /usr/local/lib/sysctl.d/.conf  
/usr/lib/sysctl.d/.conf /lib/sysctl.d/*.conf /etc/sysctl.conf`

#### **Rationale:**

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

User namespaces are used primarily for Linux container. The value 0 disallows the use of user namespaces. When containers are not in use, namespaces should be disallowed. When containers are deployed on a system, the value should be set to a large non-zero value. The default value is 7182.

#### **Impact:**

User namespaces are used primarily for Linux containers. If containers are in use, this requirement is not applicable.



**Audit:**

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `user.max_user_namespaces` is set to 0

**Note:**

- User namespaces are used primarily for Linux containers. If containers are in use, this requirement is not applicable.
- kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); a_parlist=(user.max_user_namespaces=0)
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F='/' ^\s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F='{' {print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\"")
            "    in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"") \
            "    in the running configuration" \
            "    and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="$l_out// # /}"
                else
                    l_kpar="$(awk -F='{' {print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_file")
                fi
            fi
            done < <("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([\^#\n\r]+|\#\h*\[/[\^#\n\r\h]+\.\conf\b)')
            if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
                l_kpar="$(grep -Po "^\h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
                l_kpar="$l_kpar//\./."
                [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_ufwscf")
            fi
            if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
                while IFS="" read -r l_fkpname l_file_parameter_value; do
                    l_fkpname="$l_fkpname// /}";
l_file_parameter_value="$l_file_parameter_value// /}"
                    if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_file_parameter_value"; then
                        a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\"") \
                        "    in \"$(printf '%s' "${A_out[@]}")\"")
                    else
                        a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\"") \
                        "    in \"$(printf '%s' "${A_out[@]}")\"") \
                        "    and should have a value of: \"$l_value_out\"")
                    fi
                done
            fi
        }
    }
}

```

```

done < <(grep -Po -- "\h*$l_parameter_name\h*=\h*\H+"
"${A_out[@]}")
else
a_output2+=(" - \"$l_parameter_name\" is not set in an included
file" \
    ** Note: \"$l_parameter_name\" May be set in a file that's
ignored by load procedure **)
fi
}
l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
while IFS="=" read -r l_parameter_name l_parameter_value; do # Assess and
check parameters
l_parameter_name="${l_parameter_name// /}";
l_parameter_value="${l_parameter_value// /}"
l_value_out="${l_parameter_value//-/ through }";
l_value_out="${l_value_out//|/ or }"
l_value_out="$(tr -d '()' <<< "$l_value_out")"
f_kernel_parameter_chk
done < <(printf '%s\n' "${a_parlist[@]}")
if [ "${#a_output2[@]}" -le 0 ]; then
printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
else
printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
[ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:"
"${a_output[@]}" ""
fi
}

```

## Remediation:

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `user.max_user_namespaces = 0`

### Example:

```
# printf "%s\n" "user.max_user_namespaces = 0" >> /etc/sysctl.d/60-
user_sysctl.conf
```

Run the following command to set the active kernel parameter:

```
# sysctl -w user.max_user_namespaces=0
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## Default Value:

`user.max_user_namespaces=14382`

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230548  
Rule ID: SV-230548r858828  
STIG ID: RHEL-08-040284  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## *1.5.12 Ensure kernel image loading is disabled (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system must prevent the loading of a new kernel for later execution.

### **Rationale:**

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Disabling `kexec_load` prevents an unsigned kernel image (that could be a windows kernel or modified vulnerable kernel) from being loaded. Kexec can be used subvert the entire secureboot process and should be avoided at all costs especially since it can load unsigned kernel images.

### **Audit:**

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `kernel.kexec_load_disabled` is set to **1**

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); a_parlist=(kernel.kexec_load_disabled=1)
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F= '{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\"")
            "      in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"") \
            "      in the running configuration" \
            "      and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="$l_out// # /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_file")
                fi
            fi
            done < <("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([\^#\n\r]+|\#\h*\[/[\^#\n\r\h]+\.\conf\b)')
            if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
                l_kpar="$(grep -Po "^\h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
                l_kpar="$l_kpar//\./}"
                [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_ufwscf")
            fi
            if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
                while IFS="" read -r l_fkpname l_file_parameter_value; do
                    l_fkpname="$l_fkpname// /}";
                    l_file_parameter_value="$l_file_parameter_value// /}"
                    if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_file_parameter_value"; then
                        a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\"") \
                        "      in \"$(printf '%s' "${A_out[@]}")\"")
                    else
                        a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\"") \
                        "      in \"$(printf '%s' "${A_out[@]}")\"") \
                        "      and should have a value of: \"$l_value_out\"")
                    fi
                done
            fi
        }
    }
}

```

```

done < <(grep -Po -- "\^h*$l_parameter_name\h*=\h*\H+"
"${A_out[@]}")
else
a_output2+=(" - \"$l_parameter_name\" is not set in an included
file" \
    ** Note: \"$l_parameter_name\" May be set in a file that's
ignored by load procedure **)
fi
}
l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
while IFS="=" read -r l_parameter_name l_parameter_value; do # Assess and
check parameters
l_parameter_name="${l_parameter_name// /}";
l_parameter_value="${l_parameter_value// /}"
l_value_out="${l_parameter_value//-/ through }";
l_value_out="${l_value_out//|/ or }"
l_value_out="$(tr -d '()' <<< "$l_value_out")"
f_kernel_parameter_chk
done < <(printf '%s\n' "${a_parlist[@]}")
if [ "${#a_output2[@]}" -le 0 ]; then
printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
else
printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
[ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:"
"${a_output[@]}" ""
fi
}

```

## Remediation:

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `kernel.kexec_load_disabled = 1`

### Example:

```
# printf '\n%s' "kernel.kexec_load_disabled = 1" >> /etc/sysctl.d/60-
kernel_sysctl.conf
```

Run the following command to set the active kernel parameter:

```
# sysctl -w kernel.kexec_load_disabled=1
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## Default Value:

`kernel.kexec_load_disabled = 0`

## References:

1. NIST SP 800-53 Revision 4 :: CM-5 (3)

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230266  
Rule ID: SV-230266r877463  
STIG ID: RHEL-08-010372  
Severity: CAT II

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |



### *1.5.13 Ensure the operating system is configured to enable DAC on symlinks (Automated)*

**Profile Applicability:**

- STIG

**Description:**

The operating system must enable kernel parameters to enforce discretionary access control on symlinks.

**Rationale:**

Discretionary Access Control (DAC) is based on the notion that individual users are "owners" of objects and therefore have discretion over who should be authorized to access the object and in which mode (e.g., read or write). Ownership is usually acquired as a consequence of creating the object or via specified ownership assignment. DAC allows the owner to determine who will have access to objects they control. An example of DAC includes user-controlled file permissions.

When discretionary access control policies are implemented, subjects are not constrained with regard to what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing (i.e., the subjects have the discretion to pass) the information to other subjects or objects. A subject that is constrained in its operation by Mandatory Access Control policies is still able to operate under the less rigorous constraints of this requirement. Thus, while Mandatory Access Control imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level, this requirement permits the subject to pass the information to any subject at the same sensitivity level. The policy is bounded by the information system boundary. Once the information is passed outside the control of the information system, additional means may be required to ensure the constraints remain in effect. While the older, more traditional definitions of discretionary access control require identity-based access control, that limitation is not required for this use of discretionary access control.

By enabling the `fs.protected_symlinks` kernel parameter, symbolic links are permitted to be followed only when outside a sticky world-writable directory, or when the UID of the link and follower match, or when the directory owner matches the symlink's owner. Disallowing such symlinks helps mitigate vulnerabilities based on insecure file system accessed by privileged programs, avoiding an exploitation vector exploiting unsafe use of `open()` or `creat()`.

Satisfies: SRG-OS-000312-GPOS-00122, SRG-OS-000312-GPOS-00123, SRG-OS-000312-GPOS-00124, SRG-OS-000324-GPOS-00125

**Audit:**

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `fs.protected_symlinks` is set to `1`

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); a_parlist=(fs.protected_symlinks=1)
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F= '{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\"")
            "    in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"") \
            "    in the running configuration" \
            "    and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="$l_out// # /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_file")
                fi
            fi
            done < <("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([\^#\n\r]+|\#\h*\[/\^#\n\r\h]+\.\conf\b)')
            if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
                l_kpar="$(grep -Po "^\h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
                l_kpar="$l_kpar//\./."
                [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_ufwscf")
            fi
            if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
                while IFS="" read -r l_fkpname l_file_parameter_value; do
                    l_fkpname="$l_fkpname// /}";
                    l_file_parameter_value="$l_file_parameter_value// /}"
                    if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_file_parameter_value"; then
                        a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\"") \
                        "    in \"$(printf '%s' "${A_out[@]}")\"")
                    else
                        a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\"") \
                        "    in \"$(printf '%s' "${A_out[@]}")\"") \
                        "    and should have a value of: \"$l_value_out\"")
                    fi
                done
            fi
        }
    }
}

```

```

done < <(grep -Po -- "\^h*$l_parameter_name\h*=\h*\H+"
"${A_out[@]}")
else
a_output2+=(" - \"$l_parameter_name\" is not set in an included
file" \
    ** Note: \"$l_parameter_name\" May be set in a file that's
ignored by load procedure **)
fi
}
l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
while IFS="=" read -r l_parameter_name l_parameter_value; do # Assess and
check parameters
l_parameter_name="${l_parameter_name// /}";
l_parameter_value="${l_parameter_value// /}"
l_value_out="${l_parameter_value//-/ through }";
l_value_out="${l_value_out//|/ or }"
l_value_out="$(tr -d '(){}' <<< "$l_value_out")"
f_kernel_parameter_chk
done < <(printf '%s\n' "${a_parlist[@]}")
if [ "${#a_output2[@]}" -le 0 ]; then
printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
else
printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
[ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:"
"${a_output[@]}" ""
fi
}

```

## Remediation:

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `fs.protected_symlinks = 1`

### Example:

```
# printf "%s\n" "fs.protected_symlinks = 1" >> /etc/sysctl.d/60-
fs_sysctl.conf
```

Run the following command to set the active kernel parameter:

```
# sysctl -w fs.protected_symlinks=1
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## Default Value:

`fs.protected_symlinks = 1`

## References:

1. NIST SP 800-53 Revision 5 :: AC-3 (4)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230267  
Rule ID: SV-230267r858751  
STIG ID: RHEL-08-010373  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## 1.5.14 Ensure the operating system is configured to boot to the command line (Manual)

### Profile Applicability:

- STIG

### Description:

The graphical display manager must not be installed unless it is approved.

### Rationale:

Internet services that are not required for system or application processes must not be active to decrease the attack surface of the system. Graphical display managers have a long history of security vulnerabilities and must not be used, unless approved and documented.

### Audit:

Run the following command to verify that the system is configured to boot to the command line:

```
# systemctl get-default  
  
multi-user.target
```

### Remediation:

Document the requirement for a graphical user interface with the ISSO or reinstall the operating system without the graphical user interface.

If reinstallation is not feasible, open an SSH session and run the following commands:

```
# systemctl set-default multi-user.target
```

A reboot is required for the changes to take effect.

### References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-251718  
Rule ID: SV-251718r809378  
STIG ID: RHEL-08-040321  
Severity: CAT II

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### *1.5.15 Ensure the operating system is configured to enable DAC on hardlinks (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must enable kernel parameters to enforce discretionary access control on hardlinks.

#### **Rationale:**

Discretionary Access Control (DAC) is based on the notion that individual users are "owners" of objects and therefore have discretion over who should be authorized to access the object and in which mode (e.g., read or write). Ownership is usually acquired as a consequence of creating the object or via specified ownership assignment. DAC allows the owner to determine who will have access to objects they control. An example of DAC includes user-controlled file permissions.

When discretionary access control policies are implemented, subjects are not constrained with regard to what actions they can take with information for which they have already been granted access. Thus, subjects that have been granted access to information are not prevented from passing (i.e., the subjects have the discretion to pass) the information to other subjects or objects. A subject that is constrained in its operation by Mandatory Access Control policies is still able to operate under the less rigorous constraints of this requirement. Thus, while Mandatory Access Control imposes constraints preventing a subject from passing information to another subject operating at a different sensitivity level, this requirement permits the subject to pass the information to any subject at the same sensitivity level. The policy is bounded by the information system boundary. Once the information is passed outside the control of the information system, additional means may be required to ensure the constraints remain in effect. While the older, more traditional definitions of discretionary access control require identity-based access control, that limitation is not required for this use of discretionary access control.

By enabling the `fs.protected_hardlinks` kernel parameter, users can no longer create soft or hard links to files they do not own. Disallowing such hardlinks mitigate vulnerabilities based on insecure file system accessed by privileged programs, avoiding an exploitation vector exploiting unsafe use of `open()` or `creat()`.

Satisfies: SRG-OS-000312-GPOS-00122, SRG-OS-000312-GPOS-00123, SRG-OS-000312-GPOS-00124, SRG-OS-000324-GPOS-00125



**Audit:**

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `fs.protected_hardlinks` is set to `1`

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); a_parlist=(fs.protected_hardlinks=1)
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F= '{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\"")
            "    in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"") \
            "    in the running configuration" \
            "    and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="$l_out// # /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=(["$l_kpar"]="$l_file")
                fi
            fi
            done < <("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([\^#\n\r]+|\#\h*\[/\^#\n\r\h]+\.\conf\b)')
            if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
                l_kpar="$(grep -Po "^\h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
                l_kpar="$l_kpar//\./."
                [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=(["$l_kpar"]="$l_ufwscf")
            fi
            if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
                while IFS="" read -r l_fkpname l_file_parameter_value; do
                    l_fkpname="$l_fkpname// /}";
                    l_file_parameter_value="$l_file_parameter_value// /}"
                    if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_file_parameter_value"; then
                        a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\"") \
                        "    in \"$(printf '%s' "${A_out[@]}")\"")
                    else
                        a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\"") \
                        "    in \"$(printf '%s' "${A_out[@]}")\"") \
                        "    and should have a value of: \"$l_value_out\"")
                    fi
                done
            fi
        }
    }
}

```

```

done < <(grep -Po -- "\^h*$l_parameter_name\h*=\h*\H+"
"${A_out[@]}")
else
a_output2+=(" - \"$l_parameter_name\" is not set in an included
file" \
    ** Note: \"$l_parameter_name\" May be set in a file that's
ignored by load procedure **)
fi
}
l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
while IFS="=" read -r l_parameter_name l_parameter_value; do # Assess and
check parameters
l_parameter_name="${l_parameter_name// /}";
l_parameter_value="${l_parameter_value// /}"
l_value_out="${l_parameter_value//-/ through }";
l_value_out="${l_value_out//|/ or }"
l_value_out="$(tr -d '(){}' <<< "$l_value_out")"
f_kernel_parameter_chk
done < <(printf '%s\n' "${a_parlist[@]}")
if [ "${#a_output2[@]}" -le 0 ]; then
printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
else
printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
[ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:"
"${a_output[@]}" ""
fi
}

```

## Remediation:

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `fs.protected_hardlinks = 1`

### Example:

```
# printf '\n%s' "fs.protected_hardlinks = 1" >> /etc/sysctl.d/60-
fs_sysctl.conf
```

Run the following command to set the active kernel parameter:

```
# sysctl -w fs.protected_hardlinks=1
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## Default Value:

`fs.protected_hardlinks = 1`

## References:

1. NIST SP 800-53 Revision 5 :: AC-3 (4)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230268  
Rule ID: SV-230268r858754  
STIG ID: RHEL-08-010374  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## 1.5.16 Ensure the operating system restricts exposed kernel pointer addresses access (Automated)

### Profile Applicability:

- STIG

### Description:

The operating system must restrict exposed kernel pointer addresses access.

The `sysctl --system` command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored.

`/etc/sysctl.d/.conf /run/sysctl.d/.conf /usr/local/lib/sysctl.d/.conf /usr/lib/sysctl.d/.conf /lib/sysctl.d/*.conf /etc/sysctl.conf`

### Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

### Audit:

Verify the operating system restricts exposed kernel pointer addresses access with the following commands:

```
# sysctl kernel.kptr_restrict
kernel.kptr_restrict = 1
```

If the returned line does not have a value of "1", or "2", or a line is not returned, this is a finding.

Check that the configuration files are present to enable this network parameter:

```
# grep -r kernel.kptr_restrict /run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf /etc/sysctl.d/*.conf
/etc/sysctl.d/99-sysctl.conf: kernel.kptr_restrict = 1
```

If "kernel.kptr\_restrict" is not set to "1" or "2", is missing or commented out, this is a finding.

## Remediation:

Configure the operating system to restrict exposed kernel pointer addresses access by adding the following line to a file in the "/etc/sysctl.d" directory:

```
kernel.kptr_restrict = 1
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf
/lib/sysctl.d/*.conf
/etc/sysctl.conf
/etc/sysctl.d/*.conf
```

The system configuration files need to be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
# sysctl --system
```

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230547  
Rule ID: SV-230547r858826  
STIG ID: RHEL-08-040283  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      | ●    | ●    |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      | ●    | ●    |

### *1.5.17 Ensure the operating system is configured to restrict access to the kernel message buffer (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must restrict access to the kernel message buffer.

#### **Rationale:**

Preventing unauthorized information transfers mitigates the risk of information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection.

This requirement generally applies to the design of an information technology product, but it can also apply to the configuration of particular information system components that are, or use, such products. This can be verified by acceptance/validation processes in DoD or other government agencies.

There may be shared resources with configurable protections (e.g., files in storage) that may be assessed on specific information system components.

Restricting access to the kernel message buffer limits access to only root. This prevents attackers from gaining additional system information as a non-privileged user.

#### **Audit:**

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `kernel.dmesg_restrict` is set to **1**

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); a_parlist=(kernel.dmesg_restrict=1)
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F= '{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\"")
            "      in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"") \
            "      in the running configuration" \
            "      and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="$l_out// # /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_file")
                fi
            fi
            done < <("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([\^#\n\r]+|\#\h*\[/[\^#\n\r\h]+\.\conf\b)')
            if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
                l_kpar="$(grep -Po "^\h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
                l_kpar="$l_kpar//\./}"
                [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_ufwscf")
            fi
            if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
                while IFS="" read -r l_fkpname l_file_parameter_value; do
                    l_fkpname="$l_fkpname// /}";
                    l_file_parameter_value="$l_file_parameter_value// /}"
                    if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_file_parameter_value"; then
                        a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\"") \
                        "      in \"$(printf '%s' "${A_out[@]}")\"")
                    else
                        a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\"") \
                        "      in \"$(printf '%s' "${A_out[@]}")\"") \
                        "      and should have a value of: \"$l_value_out\"")
                    fi
                done
            fi
        }
    }
}

```



```

done < <(grep -Po -- "\h*$l_parameter_name\h*=\h*\H+"
"${A_out[@]}")
else
a_output2+=(" - \"$l_parameter_name\" is not set in an included
file" \
    ** Note: \"$l_parameter_name\" May be set in a file that's
ignored by load procedure **)
fi
}
l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
while IFS="=" read -r l_parameter_name l_parameter_value; do # Assess and
check parameters
l_parameter_name="${l_parameter_name// /}";
l_parameter_value="${l_parameter_value// /}"
l_value_out="${l_parameter_value//-/ through }";
l_value_out="${l_value_out//|/ or }"
l_value_out="$(tr -d '(){}' <<< "$l_value_out")"
f_kernel_parameter_chk
done < <(printf '%s\n' "${a_parlist[@]}")
if [ "${#a_output2[@]}" -le 0 ]; then
printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
else
printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
[ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:"
"${a_output[@]}" ""
fi
}

```

## Remediation:

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `kernel.dmesg_restrict = 1`

### Example:

```
# printf '\n%s' "kernel.dmesg_restrict = 1" >> /etc/sysctl.d/60-
kernel_sysctl.conf
```

Run the following command to set the active kernel parameter:

```
# sysctl -w kernel.dmesg_restrict=1
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## Default Value:

`kernel.dmesg_restrict = 1`

## References:

1. NIST SP 800-53 Revision 5 :: SC-4
2. NIST SP 800-53A :: SC-4.1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230269  
Rule ID: SV-230269r858756  
STIG ID: RHEL-08-010375  
Severity: CAT III

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## 1.5.18 Ensure the operating system disables core dumps for all users (Automated)

### Profile Applicability:

- STIG

### Description:

The operating system must disable core dumps for all users.

### Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems.

### Audit:

Verify the operating system disables core dumps for all users by issuing the following command:

```
# grep -r -s '^[^#].*core' /etc/security/limits.conf  
/etc/security/limits.d/*.conf  
  
* hard core 0
```

This can be set as a global domain (with the \* wildcard) but may be set differently for multiple domains.

If the "core" item is missing, commented out, or the value is anything other than "0" and the need for core dumps is not documented with the Information System Security Officer (ISSO) as an operational requirement for all domains that have the "core" item assigned, this is a finding.

### Remediation:

Configure the operating system to disable core dumps for all users.

Add the following line to the top of the "/etc/security/limits.conf" file or in a ".conf" file defined in "/etc/security/limits.d/":

```
* hard core 0
```

### References:

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230313  
Rule ID: SV-230313r627750  
STIG ID: RHEL-08-010673  
Severity: CAT II

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### *1.5.19 Ensure the operating system is configured to prevent kernel profiling by unprivileged users (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must prevent kernel profiling by unprivileged users.

#### **Rationale:**

Preventing unauthorized information transfers mitigates the risk of information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection.

This requirement generally applies to the design of an information technology product, but it can also apply to the configuration of particular information system components that are, or use, such products. This can be verified by acceptance/validation processes in DoD or other government agencies.

There may be shared resources with configurable protections (e.g., files in storage) that may be assessed on specific information system components.

Setting the `kernel.perf_event_paranoid` kernel parameter to "2" prevents attackers from gaining additional system information as a non-privileged user.

#### **Audit:**

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `kernel.perf_event_paranoid` is set to 2

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); a_parlist=(kernel.perf_event_paranoid=2)
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F= '{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\"")
            "      in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"") \
            "      in the running configuration" \
            "      and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="$l_out// # /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=(["$l_kpar"]="$l_file")
                fi
            fi
            done < <("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([\^#\n\r]+|\#\h*\[/[\^#\n\r\h]+\.\conf\b)')
            if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
                l_kpar="$(grep -Po "^\h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
                l_kpar="$l_kpar//\./."
                [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=(["$l_kpar"]="$l_ufwscf")
            fi
            if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
                while IFS="" read -r l_fkpname l_file_parameter_value; do
                    l_fkpname="$l_fkpname// /}";
l_file_parameter_value="$l_file_parameter_value// /}"
                    if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_file_parameter_value"; then
                        a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\"") \
                        "      in \"$(printf '%s' "${A_out[@]}")\"")
                    else
                        a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\"") \
                        "      in \"$(printf '%s' "${A_out[@]}")\"") \
                        "      and should have a value of: \"$l_value_out\"")
                    fi
                done
            fi
        }
    }
}

```

```

done < <(grep -Po -- "\h*$l_parameter_name\h*=\h*\H+"
"${A_out[@]}")
else
a_output2+=(" - \"$l_parameter_name\" is not set in an included
file" \
    ** Note: \"$l_parameter_name\" May be set in a file that's
ignored by load procedure **)
fi
}
l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
while IFS="=" read -r l_parameter_name l_parameter_value; do # Assess and
check parameters
l_parameter_name="${l_parameter_name// /}";
l_parameter_value="${l_parameter_value// /}"
l_value_out="${l_parameter_value//-/ through }";
l_value_out="${l_value_out//|/ or }"
l_value_out="$(tr -d '()' <<< "$l_value_out")"
f_kernel_parameter_chk
done < <(printf '%s\n' "${a_parlist[@]}")
if [ "${#a_output2[@]}" -le 0 ]; then
printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
else
printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
[ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:"
"${a_output[@]}" ""
fi
}

```

## Remediation:

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `kernel.perf_event_paranoid = 2`

### Example:

```
# printf '\n%s' "kernel.perf_event_paranoid = 2" >> /etc/sysctl.d/60-
kernel_sysctl.conf
```

Run the following command to set the active kernel parameter:

```
# sysctl -w kernel.perf_event_paranoid=2
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## Default Value:

`kernel.perf_event_paranoid = 2`

## References:

1. NIST SP 800-53 Revision 5 :: SC-4
2. NIST SP 800-53A :: SC-4.1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230270  
Rule ID: SV-230270r858758  
STIG ID: RHEL-08-010376  
Severity: CAT III

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |



## 1.5.20 Ensure the operating system restricts usage of ptrace to descendant processes (Automated)

### Profile Applicability:

- STIG

### Description:

The `ptrace()` system call provides a means by which one process (the "tracer") may observe and control the execution of another process (the "tracee"), and examine and change the tracee's memory and registers.

The sysctl settings (writable only with CAP\_SYS\_PTRACE) are:

- **0** - classic ptrace permissions: a process can `PTRACE_ATTACH` to any other process running under the same uid, as long as it is dumpable (i.e. did not transition uids, start privileged, or have called `prctl(PR_SET_DUMPABLE...)` already). Similarly, `PTRACE_TRACEME` is unchanged.
- **1** - restricted ptrace: a process must have a predefined relationship with the inferior it wants to call `PTRACE_ATTACH` on. By default, this relationship is that of only its descendants when the above classic criteria is also met. To change the relationship, an inferior can call `prctl(PR_SET_PTRACER, debugger, ...)` to declare an allowed debugger PID to call `PTRACE_ATTACH` on the inferior. Using `PTRACE_TRACEME` is unchanged.
- **2** - admin-only attach: only processes with `CAP_SYS_PTRACE` may use ptrace with `PTRACE_ATTACH`, or through children calling `PTRACE_TRACEME`.
- **3** - no attach: no processes may use ptrace with `PTRACE_ATTACH` nor via `PTRACE_TRACEME`. Once set, this sysctl value cannot be changed.

### Rationale:

If one application is compromised, it would be possible for an attacker to attach to other running processes (e.g. Bash, Firefox, SSH sessions, GPG agent, etc) to extract additional credentials and continue to expand the scope of their attack.

Enabling restricted mode will limit the ability of a compromised process to `PTRACE_ATTACH` on other processes running under the same user. With restricted mode, ptrace will continue to work with root user.

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

**Audit:**

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `kernel.yama.ptrace_scope` is set to a value of: **1**

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); a_parlist=("kernel.yama.pttrace_scope=1")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F= '{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\"")
            "    in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"") \
            "    in the running configuration" \
            "    and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="$l_out// # /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_file")
                fi
            fi
            done < <("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([\^#\n\r]+|\#\h*\[/[\^#\n\r\h]+\.\conf\b)')
            if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
                l_kpar="$(grep -Po "^\h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
                l_kpar="$l_kpar//\./."
                [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_ufwscf")
            fi
            if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
                while IFS="" read -r l_fkpname l_file_parameter_value; do
                    l_fkpname="$l_fkpname// /}";
                    l_file_parameter_value="$l_file_parameter_value// /}"
                    if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_file_parameter_value"; then
                        a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\"") \
                        "    in \"$(printf '%s' "${A_out[@]}")\"")
                    else
                        a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\"") \
                        "    in \"$(printf '%s' "${A_out[@]}")\"") \
                        "    and should have a value of: \"$l_value_out\"")
                    fi
                done
            fi
        }
    }
}

```

```

done < <(grep -Po -- "\h*$l_parameter_name\h*=\h*\H+"
"${A_out[@]}")
else
a_output2+=(" - \"$l_parameter_name\" is not set in an included
file" \
    ** Note: \"$l_parameter_name\" May be set in a file that's
ignored by load procedure **)
fi
}
l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
while IFS="=" read -r l_parameter_name l_parameter_value; do # Assess and
check parameters
l_parameter_name="${l_parameter_name// /}";
l_parameter_value="${l_parameter_value// /}"
l_value_out="${l_parameter_value//-/ through }";
l_value_out="${l_value_out//|/ or }"
l_value_out="$(tr -d '()' {} ' <<< \"$l_value_out\" )"
f_kernel_parameter_chk
done < <(printf '%s\n' "${a_parlist[@]}")
if [ "${#a_output2[@]}" -le 0 ]; then
printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
else
printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
[ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:"
"${a_output[@]}" ""
fi
}

```

## Remediation:

Set the **kernel.yama.ptrace\_scope** parameter in **/etc/sysctl.conf** or a file in **/etc/sysctl.d/** ending in **.conf** to a value of **1**:

```
kernel.yama.ptrace_scope = 1
```

### Example:

```
# printf "%s\n" "kernel.yama.ptrace_scope = 1" >> /etc/sysctl.d/60-
kernel_sysctl.conf
```

Run the following command to set the active kernel parameter:

```
# sysctl -w kernel.yama.ptrace_scope=1
```

**Note:** If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten

## Default Value:

kernel.yama.ptrace\_scope = 0

## References:

1. <https://www.kernel.org/doc/Documentation/security/Yama.txt>
2. <https://github.com/raj3shp/termspy>
3. NIST SP 800-53 :: CM-6 b
4. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Ptrace is very rarely used by regular applications and is mostly used by debuggers such as **gdb** and **strace**.

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230546  
Rule ID: SV-230546r858824  
STIG ID: RHEL-08-040282  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1055, T1055.008            | TA0005  | M1040       |

*1.5.21 Ensure the operating system prevents privilege escalation through the kernel by disabling access to the bpf syscall (Automated)*

**Profile Applicability:**

- STIG

**Description:**

The operating system must disable access to network bpf syscall from unprivileged processes.

**Rationale:**

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

## Audit:

Verify, the operating system prevents privilege escalation thru the kernel by disabling access to the bpf syscall with the following commands:

```
# sysctl kernel.unprivileged_bpf_disabled  
  
kernel.unprivileged_bpf_disabled = 1
```

If the returned line does not have a value of "1", or a line is not returned, this is a finding.

Check that the configuration files are present to enable this network parameter.

```
# grep -r kernel.unprivileged_bpf_disabled /run/sysctl.d/*.conf  
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf  
/etc/sysctl.conf /etc/sysctl.d/*.conf  
  
/etc/sysctl.d/99-sysctl.conf: kernel.unprivileged_bpf_disabled = 1
```

If "kernel.unprivileged\_bpf\_disabled" is not set to "1", is missing or commented out, this is a finding.

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- **kernel.unprivileged\_bpf\_disabled** is set to **1**

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); a_parlist=(kernel.unprivileged_bpf_disabled=1)
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F= '{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\"")
            "    in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"") \
            "    in the running configuration" \
            "    and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="$l_out// # /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_file")
                fi
            fi
            done < <("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([\^#\n\r]+|\#\h*\[/[\^#\n\r\h]+\.\conf\b)')
            if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
                l_kpar="$(grep -Po '^ \h*$l_parameter_name\b' "$l_ufwscf" | xargs)"
                l_kpar="$l_kpar//\./."
                [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_ufwscf")
            fi
            if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
                while IFS="" read -r l_fkpname l_file_parameter_value; do
                    l_fkpname="$l_fkpname// /}";
                    l_file_parameter_value="$l_file_parameter_value// /}"
                    if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_file_parameter_value"; then
                        a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\"") \
                        "    in \"$(printf '%s' "${A_out[@]}")\"")
                    else
                        a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\"") \
                        "    in \"$(printf '%s' "${A_out[@]}")\"") \
                        "    and should have a value of: \"$l_value_out\"")
                    fi
                done
            fi
        }
    }
}

```



```

done < <(grep -Po -- "\h*$l_parameter_name\h*=\h*\H+"
"${A_out[@]}")
else
a_output2+=(" - \"$l_parameter_name\" is not set in an included
file" \
    ** Note: \"$l_parameter_name\" May be set in a file that's
ignored by load procedure **)
fi
}
l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
while IFS="=" read -r l_parameter_name l_parameter_value; do # Assess and
check parameters
l_parameter_name="${l_parameter_name// /}";
l_parameter_value="${l_parameter_value// /}"
l_value_out="${l_parameter_value//-/ through }";
l_value_out="${l_value_out//|/ or }"
l_value_out="$(tr -d '()' <<< "$l_value_out")"
f_kernel_parameter_chk
done < <(printf '%s\n' "${a_parlist[@]}")
if [ "${#a_output2[@]}" -le 0 ]; then
printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
else
printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
[ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:"
"${a_output[@]}" ""
fi
}

```

## Remediation:

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `kernel.unprivileged_bpf_disabled = 1`

### Example:

```
# printf '\n%s' "kernel.unprivileged_bpf_disabled = 1" >> /etc/sysctl.d/60-
kernel_sysctl.conf
```

Run the following command to set the active kernel parameter:

```
# sysctl -w kernel.unprivileged_bpf_disabled=1
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230545  
Rule ID: SV-230545r858822  
STIG ID: RHEL-08-040281  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## 1.5.22 Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed (Automated)

### Profile Applicability:

- STIG

### Description:

The x86 Ctrl-Alt-Delete key sequence must be disabled.

### Rationale:

A locally logged-on user, who presses Ctrl-Alt-Delete when at the console, can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot. In a graphical user environment, risk of unintentional reboot from the Ctrl-Alt-Delete sequence is reduced because the user will be prompted before any action is taken.

### Audit:

Verify the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed with the following command:

```
# systemctl status ctrl-alt-del.target

ctrl-alt-del.target
Loaded: masked (Reason: Unit ctrl-alt-del.target is masked.)
Active: inactive (dead)
```

If the "ctrl-alt-del.target" is loaded and not masked, this is a finding.

### Remediation:

Configure the system to disable the Ctrl-Alt-Delete sequence for the command line with the following command:

```
# systemctl disable ctrl-alt-del.target
# systemctl mask ctrl-alt-del.target
```

Created symlink /etc/systemd/system/ctrl-alt-del.target -> /dev/null  
Reload the daemon for this change to take effect.

```
# systemctl daemon-reload
```

### References:

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230529  
Rule ID: SV-230529r833338  
STIG ID: RHEL-08-040170  
Severity: CAT I

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### *1.5.23 Ensure the operating system implements the Endpoint Security for Linux Threat Prevention tool (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The Endpoint Security for Linux Threat Prevention tool must be implemented.

#### **Rationale:**

Adding endpoint security tools can provide the capability to automatically take actions in response to malicious behavior, which can provide additional agility in reacting to network threats. These tools also often include a reporting capability to provide network awareness of the system, which may not otherwise exist in an organization's systems management regime.

#### **Audit:**

Per OPOD 16-0080, the preferred endpoint security tool is McAfee Endpoint Security for Linux (ENSL) in conjunction with SELinux.

Procedure:

Check that the following package has been installed:

```
# rpm -qa | grep -i mcafeetp
```

If the "mcafeetp" package is not installed, this is a finding.

Verify that the daemon is running:

```
# ps -ef | grep -i mfetpd
```

If the daemon is not running, this is a finding.

#### **Remediation:**

Install and enable the latest McAfee ENSLTP package.

#### **References:**

1. NIST SP 800-53 :: SI-2 (2)
2. NIST SP 800-53A :: SI-2 (2).1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-245540  
Rule ID: SV-245540r942951  
STIG ID: RHEL-08-010001  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>10.5 <u>Enable Anti-Exploitation Features</u></b><br>Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.                                                                                                  |      |  |  |
| v7               | <b>8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u></b><br>Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables. |      |  |  |

## 1.6 Configure system wide crypto policy

The crypto policy definition files have a simple syntax following an INI file key = value syntax

Full policy definition files have suffix **.pol**, subpolicy files have suffix **.pmod**. Subpolicies do not have to have values set for all the keys.

The effective configuration of a policy with subpolicies applied is the same as a configuration from a single policy obtained by concatenating the policy and the subpolicies in question.

The policy files shipped in packages are placed in **/usr/share/crypto-policies/policies** and the subpolicies in **/usr/share/crypto-policies/policies/modules**.

Locally configured policy files should be placed in **/etc/crypto-policies/policies** and subpolicies in **/etc/crypto-policies/policies/modules**.

The policy and subpolicy files must have names in upper-case except for the **.pol** and **.pmod** suffix as the update-crypto-policies command always converts the policy name to upper-case before searching for the policy on the filesystem.

The following predefined policies are included:

- **DEFAULT** - The default system-wide cryptographic policy level offers secure settings for current threat models. It allows the TLS 1.2 and 1.3 protocols, as well as the IKEv2 and SSH2 protocols. The RSA keys and Diffie-Hellman parameters are accepted if they are at least 2048 bits long.
- **LEGACY** - This policy ensures maximum compatibility with Red Hat Enterprise Linux 5 and earlier; it is less secure due to an increased attack surface. In addition to the DEFAULT level algorithms and protocols, it includes support for the TLS 1.0 and 1.1 protocols. The algorithms DSA, 3DES, and RC4 are allowed, while RSA keys and Diffie-Hellman parameters are accepted if they are at least 1023 bits long.
- **FUTURE** - A stricter forward-looking security level intended for testing a possible future policy. This policy does not allow the use of SHA-1 in signature algorithms. It allows the TLS 1.2 and 1.3 protocols, as well as the IKEv2 and SSH2 protocols. The RSA keys and Diffie-Hellman parameters are accepted if they are at least 3072 bits long. If your system communicates on the public internet, you might face interoperability problems.
- **FIPS** - A policy level that conforms with the FIPS 140 requirements. The fips-mode-setup tool, which switches the RHEL system into FIPS mode, uses this policy internally. Switching to the FIPS policy does not guarantee compliance with the FIPS 140 standard. You also must re-generate all cryptographic keys after you set the system to FIPS mode. This is not possible in many scenarios.

## 1.6.1 Ensure system wide crypto policy is not set to legacy (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

When a system-wide policy is set up, the default behavior of applications will be to follow the policy. Applications will be unable to use algorithms and protocols that do not meet the policy, unless you explicitly request the application to do so.

The system-wide crypto-policies followed by the crypto core components allow consistently deprecating and disabling algorithms system-wide.

The **LEGACY** policy ensures maximum compatibility with version 5 of the operating system and earlier; it is less secure due to an increased attack surface. In addition to the **DEFAULT** level algorithms and protocols, it includes support for the **TLS 1.0** and **1.1** protocols. The algorithms **DSA**, **3DES**, and **RC4** are allowed, while **RSA keys** and **Diffie-Hellman** parameters are accepted if they are at least 1023 bits long.

### Rationale:

If the **LEGACY** system-wide crypto policy is selected, it includes support for TLS 1.0, TLS 1.1, and SSH2 protocols or later. The algorithms DSA, 3DES, and RC4 are allowed, while RSA and Diffie-Hellman parameters are accepted if larger than 1023-bits.

These legacy protocols and algorithms can make the system vulnerable to attacks, including those listed in RFC 7457

### Impact:

Environments that require compatibility with older insecure protocols may require the use of the less secure **LEGACY** policy level.

### Audit:

Run the following command to verify that the system-wide crypto policy is not **LEGACY**

```
# grep -Pi '^h*LEGACY\b' /etc/crypto-policies/config
```

Verify that no lines are returned



## Remediation:

Run the following command to change the system-wide crypto policy

```
# update-crypto-policies --set <CRYPTO POLICY>
```

*Example:*

```
# update-crypto-policies --set DEFAULT
```

Run the following to make the updated system-wide crypto policy active

```
# update-crypto-policies
```

## Default Value:

DEFAULT

## References:

1. CRYPTO-POLICIES(7)
2. <https://access.redhat.com/articles/3642912#what-polices-are-provided-1>
3. fips-mode-setup(8)
4. NIST SP 800-53 Rev. 5: SC-8

## Additional Information:

- IF - FIPS is required by local site policy:

The system-wide cryptographic policies contain a policy level that enables cryptographic algorithms in accordance with the requirements by the Federal Information Processing Standard (FIPS) Publication 140. The fips-mode-setup tool that enables or disables FIPS mode internally uses the FIPS systemwide cryptographic policy. Switching the system to FIPS mode by using the FIPS system-wide cryptographic policy does not guarantee compliance with the FIPS 140 standard. Re-generating all cryptographic keys after setting the system to FIPS mode may not be possible. For example, in the case of an existing IdM realm with users' cryptographic keys you cannot re-generate all the keys. The fips-mode-setup tool uses the FIPS policy internally. But on top of what the **update-crypto-policies** command with the **--set FIPS** option does, **fips-mode-setup** ensures the installation of the FIPS **dracut** module by using the **fips-finish-install** tool, it also adds the **fips=1** boot option to the kernel command line and regenerates the initial ramdisk.

**IMPORTANT:** Only enabling FIPS mode during installation ensures that the system generates all keys with FIPS-approved algorithms and continuous monitoring tests in place.

Run the following command to switch the system to FIPS mode:

```
# fips-mode-setup --enable
```

Output:

Kernel initramdisks are being regenerated. This might take some time.  
Setting system policy to FIPS  
Note: System-wide crypto policies are applied on application start-up.  
It is recommended to restart the system for the change of policies to fully take place.  
FIPS mode will be enabled.  
Please reboot the system for the setting to take effect.

Run the following command to restart the system:

```
# reboot
```

After the reboot has completed, run the following command to verify FIPS mode:

```
# fips-mode-setup --check
```

Output:

```
FIPS mode is enabled.
```

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                         | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |      |   |   |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                |      |  |  |

## 1.6.2 Ensure system wide crypto policy is not set in sshd configuration (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

System-wide Crypto policy can be over-ridden or opted out of for openSSH

### Rationale:

Over-riding or opting out of the system-wide crypto policy could allow for the use of less secure Ciphers, MACs, KexAlgorithms and GSSAPIKexAlgorithm

**Note:** If changes to the system-wide crypto policy are required to meet local site policy for the openSSH server, these changes should be done with a **sub-policy** assigned to the system-wide crypto policy. For additional information see the CRYPTO-POLICIES(7) man page

### Audit:

Run the following command:

```
# grep -Pi '^h*CRYPTO_POLICY\h*=' /etc/sysconfig/sshd
```

No output should be returned

### Remediation:

Run the following commands:

```
# sed -ri "s/^s*(CRYPTO_POLICY\s*=.*)$/# \1/" /etc/sysconfig/sshd
# systemctl reload sshd
```

### References:

1. NIST SP 800-53 Rev. 5: SC-8, IA-5, AC-17

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                  | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | 3.10 <u>Encrypt Sensitive Data in Transit</u><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |      | ●    | ●    |
| v7               | 14.4 <u>Encrypt All Sensitive Information in Transit</u><br>Encrypt all sensitive information in transit.                                                                                |      | ●    | ●    |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1040, T1040.000, T1557     | TA0006  | M1041       |

### 1.6.3 Ensure system wide crypto policy disables sha1 hash and signature support (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

SHA-1 (Secure Hash Algorithm) is a cryptographic hash function that produces a 160 bit hash value.

#### Rationale:

The SHA-1 hash function has an inherently weak design, and advancing cryptanalysis has made it vulnerable to attacks. The most significant danger for a hash algorithm is when a "collision" which happens when two different pieces of data produce the same hash value occurs. This hashing algorithm has been considered weak since 2005.

**Note:** The use of SHA-1 with hashbased message authentication codes (HMAC) do not rely on the collision resistance of the corresponding hash function, and therefore the recent attacks on SHA-1 have a significantly lower impact on the use of SHA-1 for HMAC. Because of this, the recommendation does not disable the hmac-sha1 MAC.

#### Audit:

Run the following commands to verify **SHA1** hash and signature support has been disabled:

Run the following command to verify that the **hash** and **sign** lines do not include the **SHA1** hash:

```
# awk -F= '($1~/ (hash|sign)/ && $2~/SHA1/ && $2!~/^\s*\-\s*([^\n\r]+)?SHA1/) {print}' /etc/crypto-policies/state/CURRENT.pol
```

Nothing should be returned

Run the following command to verify that **sha1\_in\_certs** is set to **0** (disabled):

```
# grep -Psi -- '^\h*sha1_in_certs\h*=\h*' /etc/crypto-policies/state/CURRENT.pol

sha1_in_certs = 0
```

## Remediation:

### Note:

- The commands below are written for the included **DEFAULT** system-wide crypto policy. If another policy is in use and follows local site policy, replace **DEFAULT** with the name of your system-wide crypto policy.
- Multiple subpolicies may be assigned to a policy as a colon separated list. e.g. **DEFAULT:NO-SHA1:NO-SSHCBC**
- Subpolicies:
  - Not included in the **update-crypto-policies --set** command will **not** be applied to the system wide crypto policy.
  - **must exist** before they can be applied to the system wide crypto policy.
  - **.pmod** file filenames must be in all upper case, upper case, e.g. **NO-SHA1.pmod**, or they will **not** be read by the **update-crypto-policies --set** command.

Create or edit a file in **/etc/crypto-policies/policies/modules/** ending in **.pmod** and add or modify the following lines:

```
hash = -SHA1
sign = -*SHA1
sha1_in_certs = 0
```

### Example:

```
# printf '%s\n' "# This is a subpolicy dropping the SHA1 hash and signature
support" "hash = -SHA1" "sign = -*SHA1" "sha1_in_certs = 0" >> /etc/crypto-
policies/policies/modules/NO-SHA1.pmod
```

Run the following command to update the system-wide cryptographic policy

```
# update-crypto-policies --set
<CRYPTO_POLICY>:<CRYPTO_SUBPOLICY1>:<CRYPTO_SUBPOLICY2>:<CRYPTO_SUBPOLICY3>
```

### Example:

```
update-crypto-policies --set DEFAULT:NO-SHA1
```

Run the following command to reboot the system to make your cryptographic settings effective for already running services and applications:

```
# reboot
```

## References:

1. crypto-policies(7)
2. update-crypto-policies(8)
3. Red Hat Enterprise 8 security hardening
4. <https://www.redhat.com/en/blog/how-customize-crypto-policies-rhel-82>
5. <https://access.redhat.com/articles/3642912>
6. NIST SP 800-53 Rev. 5: SC-8

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                         | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |      |  |  |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1040, T1040.000, T1557     | TA0006  | M1041       |

## 1.6.4 Ensure system wide crypto policy disables macs less than 128 bits (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Message Authentication Code (MAC) algorithm is a family of cryptographic functions that is parameterized by a symmetric key. Each of the functions can act on input data (called a “message”) of variable length to produce an output value of a specified length. The output value is called the MAC of the input message.

A MAC algorithm can be used to provide data-origin authentication and data-integrity protection

### Rationale:

Weak algorithms continue to have a great deal of attention as a weak spot that can be exploited with expanded computing power. An attacker that breaks the algorithm could take advantage of a MiTM position to decrypt the tunnel and capture credentials and information.

A MAC algorithm must be computationally infeasible to determine the MAC of a message without knowledge of the key, even if one has already seen the results of using that key to compute the MAC's of other messages.

### Audit:

Run the following script to verify weak MACs are disabled:

```
# grep -Pi -- '\h*mac\h*=\h*([\^#\n\r]+)?-64\b' /etc/crypto-  
policies/state/CURRENT.pol  
  
Nothing should be returned
```



## Remediation:

### Note:

- The commands below are written for the included **DEFAULT** system-wide crypto policy. If another policy is in use and follows local site policy, replace **DEFAULT** with the name of your system-wide crypto policy.
- Multiple subpolicies may be assigned to a policy as a colon separated list. e.g. **DEFAULT:NO-SHA1:NO-SSHCBC**
- Subpolicies:
  - Not included in the **update-crypto-policies --set** command will **not** be applied to the system wide crypto policy.
  - **must exist** before they can be applied to the system wide crypto policy.
  - **.pmod** file filenames must be in all upper case, upper case, e.g. **NO-WEAKMAC.pmod**, or they will **not** be read by the **update-crypto-policies --set** command.

Create or edit a file in **/etc/crypto-policies/policies/modules/** ending in **.pmod** and add or modify **one** of the following lines:

```
mac = --64* # Disables weak macs
```

#### Example:

```
# printf '%s\n' "# This is a subpolicy to disable weak macs" "mac = --64" >>
/etc/crypto-policies/policies/modules/NO-WEAKMAC.pmod
```

Run the following command to update the system-wide cryptographic policy

```
# update-crypto-policies --set
<CRYPTO_POLICY>:<CRYPTO_SUBPOLICY1>:<CRYPTO_SUBPOLICY2>:<CRYPTO_SUBPOLICY3>
```

#### Example:

```
update-crypto-policies --set DEFAULT:NO-SHA1:NO-WEAKMAC
```

Run the following command to reboot the system to make your cryptographic settings effective for already running services and applications:

```
# reboot
```

## References:

1. <https://nvd.nist.gov/vuln/detail/CVE-2008-5161>
2. [crypto-policies\(7\)](#)
3. [update-crypto-policies\(8\)](#)
4. Red Hat Enterprise 8 security hardening
5. <https://www.redhat.com/en/blog/how-customize-crypto-policies-rhel-82>
6. [https://csrc.nist.gov/glossary/term/message\\_authentication\\_code\\_algorithm](https://csrc.nist.gov/glossary/term/message_authentication_code_algorithm)
7. NIST SP 800-53 Rev. 5: SC-8

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                         | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |      |  |  |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1040, T1040.000, T1557     | TA0006  | M1041       |

### *1.6.5 Ensure system wide crypto policy disables cbc for ssh (Automated)*

**Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

**Description:**

Cypher Block Chaining (CBC) is an algorithm that uses a block cipher.

**Rationale:**

A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext. If exploited, this attack can potentially allow an attacker to recover up to 32 bits of plaintext from an arbitrary block of ciphertext from a connection secured using the SSH protocol.

**Impact:**

CBC ciphers might be the only common cyphers when connecting to older SSH clients and servers

## Audit:

Run the following script to verify **CBC** is disabled for **SSH**:

```
#!/usr/bin/env bash

{
    l_output="" l_output2=""
    if grep -Piq -- '^h*cipher\h*=\h*([\#\n\r]+)?-CBC\b' /etc/crypto-
policies/state/CURRENT.pol; then
        if grep -Piq -- '^h*cipher@(lib|open)ssh(-server|-client)?\h*=\h*'
/etc/crypto-policies/state/CURRENT.pol; then
            if ! grep -Piq -- '^h*cipher@(lib|open)ssh(-server|-
client)?\h*=\h*([\#\n\r]+)?-CBC\b' /etc/crypto-policies/state/CURRENT.pol;
then
                l_output="$l_output\n - Cipher Block Chaining (CBC) is disabled
for SSH"
            else
                l_output2="$l_output2\n - Cipher Block Chaining (CBC) is enabled
for SSH"
            fi
        else
            l_output2="$l_output2\n - Cipher Block Chaining (CBC) is enabled for
SSH"
        fi
    else
        l_output=" - Cipher Block Chaining (CBC) is disabled"
    fi
    if [ -z "$l_output2" ]; then # Provide output from checks
        echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
    else
        echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
    fi
}
```

## Remediation:

### Note:

- The commands below are written for the included **DEFAULT** system-wide crypto policy. If another policy is in use and follows local site policy, replace **DEFAULT** with the name of your system-wide crypto policy.
- **CBC** can be turned off globally by using the argument **cipher** opposed to **cipher@SSH**
- Multiple subpolicies may be assigned to a policy as a colon separated list. e.g. **DEFAULT:NO-SHA1:NO-SSHCBC**
- Subpolicies:
  - Not included in the **update-crypto-policies --set** command will **not** be applied to the system wide crypto policy.
  - **must exist** before they can be applied to the system wide crypto policy.
  - **.pmod** file filenames must be in all upper case, upper case, e.g. **NO-SSHCBC.pmod**, or they will **not** be read by the **update-crypto-policies --set** command.Create or edit a file in **/etc/crypto-policies/policies/modules/** ending in **.pmod** and add or modify **one** of the the following lines:

```
cipher@SSH = -*CBC # Disables the CBC cipher for SSH
```

### Example:

```
# printf '%s\n' "# This is a subpolicy to disable all CBC mode ciphers" "#  
for the SSH protocol (libssh and OpenSSH)" "cipher@SSH = -*CBC" >>  
/etc/crypto-policies/policies/modules/NO-SSHCBC.pmod
```

Run the following command to update the system-wide cryptographic policy

```
# update-crypto-policies --set  
<CRYPTO_POLICY>:<CRYPTO_SUBPOLICY1>:<CRYPTO_SUBPOLICY2>:<CRYPTO_SUBPOLICY3>
```

### Example:

```
update-crypto-policies --set DEFAULT:NO-SHA1:NO-WEAKMAC:NO-SSHCBC
```

Run the following command to reboot the system to make your cryptographic settings effective for already running services and applications:

```
# reboot
```

## References:

1. <https://nvd.nist.gov/vuln/detail/CVE-2008-5161>
2. crypto-policies(7)
3. update-crypto-policies(8)
4. Red Hat Enterprise 8 security hardening
5. <https://www.redhat.com/en/blog/how-customize-crypto-policies-rhel-82>
6. NIST SP 800-53 Rev. 5: SC-8

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                         | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |      |  |  |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1040, T1040.000, T1557     | TA0006  | M1041       |

### *1.6.6 Ensure system wide crypto policy disables chacha20-poly1305 for ssh (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

ChaCha20-Poly1305 is an authenticated encryption with additional data (AEAD) algorithm, that combines the ChaCha20 stream cipher with the Poly1305 message authentication code. Its usage in IETF protocols is standardized in RFC 8439.

#### **Rationale:**

A vulnerability exists in ChaCha20-Poly1305 as referenced in [CVE-2023-48795](#)

## Audit:

- IF - **CVE-2023-48795** has been addressed, and it meets local site policy, this recommendation may be skipped.

Run the following script to verify **chacha20-poly1305** is disabled for **SSH**:

```
#!/usr/bin/env bash

{
  l_output="" l_output2=""
  if grep -Piq -- '^\\h*cipher\\h*=\\h*([\\^#\\n\\r]+)?-CBC\\b' /etc/crypto-
policies/state/CURRENT.pol; then
    if grep -Piq -- '^\\h*cipher@(lib|open)ssh(-server|-client)?\\h*=\\h*'
/etc/crypto-policies/state/CURRENT.pol; then
      if ! grep -Piq -- '^\\h*cipher@(lib|open)ssh(-server|-
client)?\\h*=\\h*([\\^#\\n\\r]+)?\\bchacha20-poly1305\\b' /etc/crypto-
policies/state/CURRENT.pol; then
        l_output="$l_output\\n - chacha20-poly1305 is disabled for SSH"
      else
        l_output2="$l_output2\\n - chacha20-poly1305 is enabled for SSH"
      fi
    else
      l_output2="$l_output2\\n - chacha20-poly1305 is enabled for SSH"
    fi
  else
    l_output=" - chacha20-poly1305 is disabled"
  fi
  if [ -z "$l_output2" ]; then # Provide output from checks
    echo -e "\\n- Audit Result:\\n  ** PASS **\\n$l_output\\n"
  else
    echo -e "\\n- Audit Result:\\n  ** FAIL **\\n - Reason(s) for audit
failure:\\n$l_output2\\n"
    [ -n "$l_output" ] && echo -e "\\n- Correctly set:\\n$l_output\\n"
  fi
}
```



## Remediation:

### Note:

- The commands below are written for the included **DEFAULT** system-wide crypto policy. If another policy is in use and follows local site policy, replace **DEFAULT** with the name of your system-wide crypto policy.
- **chacha20-poly1305** can be turned off globally by using the argument **cipher** opposed to **cipher@SSH**
- Multiple subpolicies may be assigned to a policy as a colon separated list. e.g. **DEFAULT:NO-SHA1:NO-SSHCBC**
- Subpolicies:
  - Not included in the **update-crypto-policies --set** command will **not** be applied to the system wide crypto policy.
  - **must exist** before they can be applied to the system wide crypto policy.
  - **.pmod** file filenames must be in all upper case, upper case, e.g. **NO-SSHCACHA20.pmod**, or they will **not** be read by the **update-crypto-policies --set** command.

- IF - **CVE-2023-48795** has been addressed, and it meets local site policy, this recommendation may be skipped.

Create or edit a file in **/etc/crypto-policies/policies/modules/** ending in **.pmod** and add or modify **one** of the the following lines:

```
cipher@SSH = -CHACHA20-POLY1305 # Disables the chacha20-poly1305 cipher for SSH
```

### Example:

```
# printf '%s\n' "# This is a subpolicy to disable the chacha20-poly1305 ciphers" "# for the SSH protocol (libssh and OpenSSH)" "cipher@SSH = -CHACHA20-POLY1305" >> /etc/crypto-policies/policies/modules/NO-SSHCACHA20.pmod
```

Run the following command to update the system-wide cryptographic policy

```
# update-crypto-policies --set <CRYPTO_POLICY>:<CRYPTO_SUBPOLICY1>:<CRYPTO_SUBPOLICY2>:<CRYPTO_SUBPOLICY3>
```

### Example:

```
# update-crypto-policies --set DEFAULT:NO-SHA1:NO-WEAKMAC:NO-SSHCBC:NO-SSHCACHA20
```

Run the following command to reboot the system to make your cryptographic settings effective for already running services and applications:

```
# reboot
```

## References:

1. <https://nvd.nist.gov/vuln/detail/CVE-2023-48795>
2. crypto-policies(7)
3. update-crypto-policies(8)
4. Red Hat Enterprise 8 security hardening
5. <https://www.redhat.com/en/blog/how-customize-crypto-policies-rhel-82>
6. NIST SP 800-53 Rev. 5: SC-8

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                         | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |      |  |  |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1040, T1040.000, T1557     | TA0006  | M1041       |

## 1.6.7 Ensure system wide crypto policy disables EtM for ssh (Manual)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Encrypt-then-MAC (EtM) - The ciphertext is generated by encrypting the plaintext and then appending a MAC of the encrypted plaintext

### Rationale:

There is an effective attack against SSH's use of Cypher-Block-Chaining (CBC) with Encrypt-then-MAC as referenced in [CVE-2023-48795](#)

### Audit:

- IF - [CVE-2023-48795](#) has been addressed or if CBC is disabled for OpenSSH server this recommendation is not needed.

Run the following command to verify EtM is disabled for SSH:

```
# grep -Psi -- '^h*etm\b' /etc/crypto-policies/state/CURRENT.pol
```

Verify output includes either:

```
etm@libssh = DISABLE_ETM
etm@openssh-client = DISABLE_ETM
etm@openssh-server = DISABLE_ETM
```

- OR -

```
etm = DISABLE_ETM
```

**Note:** The ability to disable EtM through system wide crypto policy was added in version 9.3

## Remediation:

### Note:

- The commands below are written for the included **DEFAULT** system-wide crypto policy. If another policy is in use and follows local site policy, replace **DEFAULT** with the name of your system-wide crypto policy.
- **EtM** can be turned off globally by using the argument **etm** opposed to **etm@SSH**
- Multiple subpolicies may be assigned to a policy as a colon separated list. e.g. **DEFAULT:NO-SHA1:NO-SSHCBC**
- Subpolicies:
  - Not included in the **update-crypto-policies --set** command will **not** be applied to the system wide crypto policy.
  - **must exist** before they can be applied to the system wide crypto policy.
  - **.pmod** file filenames must be in all upper case, upper case, e.g. **NO-SSHCHACHA20.pmod**, or they will **not** be read by the **update-crypto-policies --set** command.

- **IF - CVE-2023-48795** has been addressed, and it meets local site policy, this recommendation may be skipped.

Create or edit a file in **/etc/crypto-policies/policies/modules/** ending in **.pmod** and add or modify the following line:

```
etm@SSH = DISABLE_ETM # This disables EtM for openSSH and libssh
```

### Example:

```
# printf '%s\n' "# This is a subpolicy to disable Encrypt then MAC" "# for the SSH protocol (libssh and OpenSSH)" "etm@SSH = DISABLE_ETM" >> /etc/crypto-policies/policies/modules/NO-SSHETM.pmod
```

Run the following command to update the system-wide cryptographic policy

```
# update-crypto-policies --set <CRYPTO_POLICY>:<CRYPTO_SUBPOLICY1>:<CRYPTO_SUBPOLICY2>:<CRYPTO_SUBPOLICY3>
```

### Example:

```
# update-crypto-policies --set DEFAULT:NO-SHA1:NO-WEAKMAC:NO-SSHCBC:NO-SSHCHACHA20:NO-SSHETM
```

Run the following command to reboot the system to make your cryptographic settings effective for already running services and applications:

```
# reboot
```

## References:

1. <https://nvd.nist.gov/vuln/detail/CVE-2023-48795>
2. crypto-policies(7)
3. update-crypto-policies(8)
4. Red Hat Enterprise 8 security hardening
5. <https://www.redhat.com/en/blog/how-customize-crypto-policies-rhel-82>
6. NIST SP 800-53 Rev. 5: SC-8
7. <https://access.redhat.com/errata/RHSA-2024:0499>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                  | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.10 Encrypt Sensitive Data in Transit</b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |      |  |  |
| v7               | <b>14.4 Encrypt All Sensitive Information in Transit</b><br>Encrypt all sensitive information in transit.                                                                                |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1040, T1040.000, T1557     | TA0006  | M1041       |

## 1.6.8 Ensure system-wide crypto policy is FIPS (Automated)

### Profile Applicability:

- STIG

### Description:

The operating system must implement NIST FIPS-validated cryptography for the following: to provision digital signatures, to generate cryptographic hashes, and to protect data requiring data-at-rest protections in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

The system-wide cryptographic policies contain a policy level that enables cryptographic algorithms in accordance with the requirements by the Federal Information Processing Standard (FIPS) Publication 140. The fips-mode-setup tool that enables or disables FIPS mode internally uses the FIPS systemwide cryptographic policy. Switching the system to FIPS mode by using the FIPS system-wide cryptographic policy does not guarantee compliance with the FIPS 140 standard. Re-generating all cryptographic keys after setting the system to FIPS mode may not be possible. For example, in the case of an existing IdM realm with users' cryptographic keys you cannot re-generate all the keys. The fips-mode-setup tool uses the FIPS policy internally. But on top of what the `update-crypto-policies` command with the `--set FIPS` option does, `fips-mode-setup` ensures the installation of the FIPS `dracut` module by using the `fips-finish-install` tool, it also adds the `fips=1` boot option to the kernel command line and regenerates the initial ramdisk.

**IMPORTANT:** Only enabling FIPS mode during installation ensures that the system generates all keys with FIPS-approved algorithms and continuous monitoring tests in place.

### Rationale:

Use of weak or untested encryption algorithms undermines the purposes of using encryption to protect data. The operating system must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000125-GPOS-00065, SRG-OS-000396-GPOS-00176, SRG-OS-000423-GPOS-00187, SRG-OS-000478-GPOS-00223

## Audit:

Run the following command to verify the system is running in FIPS mode:

```
# fips-mode-setup --check
```

Verify output includes:

```
FIPS mode is enabled
```

- **IF** - FIPS mode is **enabled**

Run the following command to verify the kernel boot parameter is configured for FIPS mode:

```
# grub2-editenv list | grep -Pso -- '\bfips=1\b'
fips=1
```

- **IF** - the kernel boot parameter is configured to use FIPS mode

Run the following command to verify the system is in FIPS mode:

```
# grep -Ps -- '^h*1\b' /proc/sys/crypto/fips_enabled
1
```

**Note:** All three audit steps need to pass to be concentrated compliant with this Recommendation

## Remediation:

Run the following command to switch the system to FIPS mode:

```
# fips-mode-setup --enable
```

Output will include:

```
FIPS mode will be enabled.  
Please reboot the system for the setting to take effect
```

Run the following command to restart the system:

```
# reboot
```

After the reboot has completed, re-run the Audit Procedure to verify FIPS mode

### Note:

- To enable strict FIPS compliance, the **fips=1** kernel option needs to be added to the kernel boot parameters during system installation so key generation is done with FIPS-approved algorithms and continuous monitoring tests in place. Users must also ensure the system has plenty of entropy during the installation process by moving the mouse around, or if no mouse is available, ensuring that many keystrokes are typed. The recommended amount of keystrokes is 256 and more. Less than 256 keystrokes may generate a nonunique key.
- RHEL 8 utilizes GRUB 2 as the default bootloader. Note that GRUB 2 command-line parameters are defined in the **kernelopts** variable of the **/boot/grub2/grubenv** file for all kernel boot entries. The command **fips-mode-setup** modifies the "kernelopts" variable, which in turn updates all kernel boot entries.
- **kernelopts** variables can be viewed with the **grubby --info=all** all command

### Default Value:

Not enabled

### References:

1. NIST SP 800-53 :: AC-17 (2)
2. NIST SP 800-53A :: AC-17 (2).1



## Additional Information:

### Red Hat Enterprise Linux 8 STIG

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230223  
RULE ID: SV-230223r928585  
STIG ID: RHEL-08-010020  
SEVERITY: CAT I

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                         | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |      |  |  |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1040, T1040.000, T1557     | TA0006  | M1041       |

### *1.6.9 Ensure PKI-based authentication has valid certificates (Manual)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must validate certificates for PKI-based authentication by constructing a certification path (which includes status information) to an accepted trust anchor.

A trust anchor is an authoritative entity represented via a public key and associated data. It is used in the context of public key infrastructures, X.509 digital certificates, and DNSSEC.

When there is a chain of trust, usually the top entity to be trusted becomes the trust anchor; it can be, for example, a Certification Authority (CA). A certification path starts with the subject certificate and proceeds through a number of intermediate certificates up to a trusted root certificate, typically issued by a trusted CA.

#### **Rationale:**

Without path validation, an informed trust decision by the relying party cannot be made when presented with any certificate not already explicitly trusted.

This Recommendation verifies that a certification path to an accepted trust anchor is used for certificate validation and that the path includes status information. Path validation is necessary for a relying party to make an informed trust decision when presented with any certificate not already explicitly trusted. Status information for certification paths includes certificate revocation lists or online certificate status protocol responses. Validation of the certificate status information is out of scope for this requirement.

Satisfies: SRG-OS-000066-GPOS-00034, SRG-OS-000384-GPOS-00167

## Audit:

Verify PKI-based authentication has valid certificates by constructing a certification path (which includes status information) to an accepted trust anchor.

Run the following command to verify the system has a valid DoD root CA installed:

```
# openssl x509 -text -in /etc/sssdpki/sssdpki_auth_ca_db.pem

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = US, O = U.S. Government, OU = DoD, OU = PKI, CN = DoD Root CA 3
Validity
Not Before: Mar 20 18:46:41 2012 GMT
Not After : Dec 30 18:46:41 2029 GMT
Subject: C = US, O = U.S. Government, OU = DoD, OU = PKI, CN = DoD Root CA 3
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
```

Verify the root ca file is a DoD-issued certificate with a valid date and installed in the "/etc/sssdpki/sssdpki\_auth\_ca\_db.pem" location.

## Remediation:

Configure PKI-based authentication to validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.

Obtain a valid copy of the DoD root CA file from the PKI CA certificate bundle from cyber.mil and copy the "DoD\_PKE\_CA\_chain.pem" into the following file:

```
/etc/sssdpki/sssdpki_auth_ca_db.pem
```

## References:

1. NIST SP 800-53 :: IA-5 (2)
2. NIST SP 800-53A :: IA-5 (2).1

## Additional Information:

Red Hat Enterprise Linux 8

Red Hat Enterprise Linux 8 STIG  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230229  
RULE ID: SV-230229r858739  
STIG ID: RHEL-08-010090  
SEVERITY: CAT II

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

## 1.6.10 Ensure system-wide crypto policies are in effect (Automated)

### Profile Applicability:

- STIG

### Description:

The SSH daemon must be configured to use system-wide crypto policies.

### Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

RHEL 8 operating systems incorporate system-wide crypto policies by default. The SSH configuration file has no effect on the ciphers, MACs, or algorithms unless specifically defined in the "/etc/sysconfig/ssh" file. The employed algorithms can be viewed in the "/etc/crypto-policies/back-ends" directory.

Satisfies: SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174, SRG-OS-000125-GPOS-00065

### Audit:

Verify that system-wide crypto policies are in effect:

```
# grep -i crypto_policy /etc/sysconfig/ssh
```

Output should be similar to:

```
# crypto_policy=
```

If the "crypto\_policy" is uncommented, this is a finding.

## Remediation:

Configure the SSH daemon to use system-wide crypto policies by adding the following line to `/etc/sysconfig/sshd`:

```
# crypto_policy=
```

A reboot is required for the changes to take effect.

## References:

1. NIST SP 800-53 :: AC-17 (2)
2. NIST SP 800-53A :: AC-17 (2).1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244526  
Rule ID: SV-244526r877394  
STIG ID: RHEL-08-010287  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                         | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |      |  |  |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                |      |  |  |

## *1.6.11 Ensure the operating system implements certificate status checking for multifactor authentication (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system must implement certificate status checking for multifactor authentication.

### **Rationale:**

Using an authentication device, such as a DoD Common Access Card (CAC) or token that is separate from the information system, ensures that even if the information system is compromised, credentials stored on the authentication device will not be affected.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification (PIV) card and the DoD CAC.

RHEL 8 operating systems include multiple options for configuring certificate status checking, but for this requirement focuses on the System Security Services Daemon (SSSD). By default, sssd performs Online Certificate Status Protocol (OCSP) checking and certificate verification using a sha256 digest function.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000377-GPOS-00162

### **Audit:**

Verify the operating system implements certificate status checking for multifactor authentication.

Check to see if Online Certificate Status Protocol (OCSP) is enabled and using the proper digest value on the system with the following command:

```
# grep certificate_verification /etc/sss/sss.conf /etc/sss/conf.d/*.conf |  
grep -v "^#"  
  
certificate_verification = ocsp_dgst=sha1
```

If the `certificate_verification` line is missing from the `[sss]` section, or is missing `"ocsp_dgst=sha1"`, ask the administrator to indicate what type of multifactor authentication is being utilized and how the system implements certificate status checking. If there is no evidence of certificate status checking being used, this is a finding.

**Remediation:**

Configure the operating system to implement certificate status checking for multifactor authentication.  
Review the "/etc/sss/sss.conf" file to determine if the system is configured to prevent OCSP or certificate verification.  
Add the following line to the "/etc/sss/sss.conf" file:

```
certificate_verification = ocsp_dgst=sha1
```

The "sss" service must be restarted for the changes to take effect. To restart the "sss" service, run the following command:

```
# systemctl restart sss.service
```

**References:**

- 1. NIST SP 800-53 Revision 4 :: IA-2 (11)

**Additional Information:**

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024  
  
Vul ID: V-230274  
Rule ID: SV-230274r858741  
STIG ID: RHEL-08-010400  
Severity: CAT II

**CIS Controls:**

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |



### *1.6.12 Ensure the OpenSSL library is configured to use only ciphers employing FIPS 140-2-approved algorithms (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must implement DoD-approved encryption in the OpenSSL package.

#### **Rationale:**

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

RHEL 8 operating systems incorporate system-wide crypto policies by default. The employed algorithms can be viewed in the `/etc/crypto-policies/back-ends/openssl.config` file.

Satisfies: SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174, SRG-OS-000125-GPOS-00065

## Audit:

Verify the OpenSSL library is configured to use only ciphers employing FIPS 140-2-approved algorithms:

Verify that system-wide crypto policies are in effect:

```
# grep -i opensslcnf.config /etc/pki/tls/openssl.cnf  
.include /etc/crypto-policies/back-ends/opensslcnf.config
```

If the "opensslcnf.config" is not defined in the "/etc/pki/tls/openssl.cnf" file, this is a finding.

Verify which system-wide crypto policy is in use:

```
# update-crypto-policies --show  
  
FIPS
```

If the system-wide crypto policy is set to anything other than "FIPS", this is a finding.

## Remediation:

Configure the OpenSSL library to use only ciphers employing FIPS 140-2-approved algorithms with the following command:

```
# fips-mode-setup --enable
```

A reboot is required for the changes to take effect.

## References:

1. NIST SP 800-53 Revision 5 :: AC-17 (2)
2. NIST SP 800-53A :: AC-17 (2).1

## Additional Information:

```
Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024  
  
Vul ID: V-230254  
Rule ID: SV-230254r877394  
STIG ID: RHEL-08-010293  
Severity: CAT II
```

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                         | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |      |  |  |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                |      |  |  |

### *1.6.13 Ensure the OpenSSL library is configured to use only DoD-approved TLS encryption (Automated)*

**Profile Applicability:**

- STIG

**Description:**

The operating system must implement DoD-approved TLS encryption in the OpenSSL package.

**Rationale:**

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

RHEL 8 operating systems incorporate system-wide crypto policies by default. The employed algorithms can be viewed in the `/etc/crypto-policies/back-ends/openssl.config` file.

Satisfies: SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174, SRG-OS-000125-GPOS-00065

## Audit:

Verify the OpenSSL library is configured to use only DoD-approved TLS encryption:  
For versions prior to crypto-policies-20210617-1.gitc776d3e.el8.noarch:

```
# grep -i MinProtocol /etc/crypto-policies/back-ends/opensslcnf.config  
MinProtocol = TLSv1.2
```

If the "MinProtocol" is set to anything older than "TLSv1.2", this is a finding.  
For version crypto-policies-20210617-1.gitc776d3e.el8.noarch and newer:

```
# grep -i MinProtocol /etc/crypto-policies/back-ends/opensslcnf.config  
  
TLS.MinProtocol = TLSv1.2  
DTLS.MinProtocol = DTLSv1.2
```

If the "TLS.MinProtocol" is set to anything older than "TLSv1.2" or the  
"DTLS.MinProtocol" is set to anything older than DTLSv1.2, this is a finding.

## Remediation:

Configure the OpenSSL library to use only DoD-approved TLS encryption by editing the  
following line in the "/etc/crypto-policies/back-ends/opensslcnf.config" file:

```
MinProtocol = TLSv1.2
```

**Note:** For version crypto-policies-20210617-1.gitc776d3e.el8.noarch and newer:

```
TLS.MinProtocol = TLSv1.2  
DTLS.MinProtocol = DTLSv1.2
```

A reboot is required for the changes to take effect.

## References:

1. NIST SP 800-53 Revision 5 :: AC-17 (2)
2. NIST SP 800-53A :: AC-17 (2).1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230255  
Rule ID: SV-230255r877394  
STIG ID: RHEL-08-010294  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                         | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |      |  |  |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                |      |  |  |

## 1.6.14 Ensure the GnuTLS library is configured to only allow DoD-approved SSL/TLS Versions (Automated)

### Profile Applicability:

- STIG

### Description:

The operating system must implement DoD-approved TLS encryption in the GnuTLS package.

### Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Transport Layer Security (TLS) encryption is a required security setting as a number of known vulnerabilities have been reported against Secure Sockets Layer (SSL) and earlier versions of TLS. Encryption of private information is essential to ensuring data confidentiality. If private information is not encrypted, it can be intercepted and easily read by an unauthorized party. SQL Server must use a minimum of FIPS 140-2-approved TLS version 1.2, and all non-FIPS-approved SSL and TLS versions must be disabled. NIST SP 800-52 specifies the preferred configurations for government systems.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

The GnuTLS library offers an API to access secure communications protocols. SSLv2 is not available in the GnuTLS library. The operating system's system-wide crypto policy defines employed algorithms in the `/etc/crypto-policies/back-ends/gnutls.config` file.

Satisfies: SRG-OS-000250-GPOS-00093, SRG-OS-000423-GPOS-00187

### Audit:

Verify the GnuTLS library is configured to only allow DoD-approved SSL/TLS Versions:

```
# grep -io +vers.* /etc/crypto-policies/back-ends/gnutls.config  
  
+VERS-ALL:-VERS-DTLS0.9:-VERS-SSL3.0:-VERS-TLS1.0:-VERS-TLS1.1:-VERS-  
DTLS1.0:+COMP=NULL:%PROFILE_MEDIUM
```

If the "gnutls.config" does not list "-VERS-DTLS0.9:-VERS-SSL3.0:-VERS-TLS1.0:-VERS-TLS1.1:VERS-DTLS1.0" to disable unapproved SSL/TLS versions, this is a finding.

## Remediation:

Configure the operating system's GnuTLS library to use only DoD-approved encryption by adding the following line to "/etc/crypto-policies/back-ends/gnutls.config":

```
+VERS-ALL:-VERS-DTLS0.9:-VERS-SSL3.0:-VERS-TLS1.0:-VERS-TLS1.1:-VERS-DTLS1.0
```

A reboot is required for the changes to take effect.

## References:

1. NIST SP 800-53 Revision 5 :: AC-17 (2)
2. NIST SP 800-53A :: AC-17 (2).1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230256  
Rule ID: SV-230256r877394  
STIG ID: RHEL-08-010295  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                  | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | 3.10 <u>Encrypt Sensitive Data in Transit</u><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |      |  |  |
| v7               | 14.4 <u>Encrypt All Sensitive Information in Transit</u><br>Encrypt all sensitive information in transit.                                                                                |      |  |  |



## 1.7 Configure Command Line Warning Banners

Presenting a warning message prior to the normal user login may assist in the prosecution of trespassers on the computer system. Changing some of these login banners also has the side effect of hiding OS version information and other detailed system information from attackers attempting to target specific exploits at a system.

Guidelines published by the US Department of Defense require that warning messages include at least the name of the organization that owns the system, the fact that the system is subject to monitoring and that such monitoring is in compliance with local statutes, and that use of the system implies consent to such monitoring. It is important that the organization's legal counsel review the content of all messages before any system modifications are made, as these warning messages are inherently site-specific. More information (including citations of relevant case law) can be found at <http://www.justice.gov/criminal/cybercrime/>

The `/etc/motd`, `/etc/issue`, and `/etc/issue.net` files govern warning banners for standard command line logins for both local and remote users.

**Note:** The text provided in the remediation actions for these items is intended as an example only. Please edit to include the specific text for your organization as approved by your legal department.

## 1.7.1 Ensure message of the day is configured properly (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The contents of the `/etc/motd` file are displayed to users after login and function as a message of the day for authenticated users.

Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If `mingetty(8)` supports the following options, they display operating system information: `\m` - machine architecture `\r` - operating system release `\s` - operating system name `\v` - operating system version

### Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the "`uname -a`" command once they have logged in.

### Audit:

Run the following command and verify that the contents match site policy:

```
# cat /etc/motd
```

Run the following command and verify no results are returned:

```
# grep -E -i "(\\v|\\r|\\m|\\s|$(grep '^ID=' /etc/os-release | cut -d= -f2 | sed -e 's/"/g'))" /etc/motd
```

## Remediation:

Edit the `/etc/motd` file with the appropriate contents according to your site policy, remove any instances of `\m` , `\r` , `\s` , `\v` or references to the `OS platform`

- OR -

- IF - the `motd` is not used, this file can be removed.

Run the following command to remove the `motd` file:

```
# rm /etc/motd
```

## References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-1, CM-3

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1082, T1082.000, T1592, T1592.004 | TA0007  |             |

## 1.7.2 Ensure local login warning banner is configured properly (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The contents of the `/etc/issue` file are displayed to users prior to login for local terminals.

Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If `mingetty(8)` supports the following options, they display operating system information: `\m` - machine architecture `\r` - operating system release `\s` - operating system name `\v` - operating system version - or the operating system's name

### Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the "`uname -a`" command once they have logged in.

### Audit:

Run the following command and verify that the contents match site policy:

```
# cat /etc/issue
```

Run the following command and verify no results are returned:

```
# grep -E -i "(\\v|\\r|\\m|\\s|$(grep '^ID=' /etc/os-release | cut -d= -f2 | sed -e 's/"/\\g'))" /etc/issue
```

## Remediation:

Edit the `/etc/issue` file with the appropriate contents according to your site policy, remove any instances of `\m`, `\r`, `\s`, `\v` or references to the **OS platform**

*Example:*

```
# echo "Authorized users only. All activity may be monitored and reported." > /etc/issue
```

## References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-1, CM-3

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1082, T1082.000, T1592, T1592.004 | TA0007  |             |

### 1.7.3 Ensure remote login warning banner is configured properly (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The contents of the `/etc/issue.net` file are displayed to users prior to login for remote connections from configured services.

Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If `mingetty(8)` supports the following options, they display operating system information: `\m` - machine architecture `\r` - operating system release `\s` - operating system name `\v` - operating system version

#### Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the "`uname -a`" command once they have logged in.

#### Audit:

Run the following command and verify that the contents match site policy:

```
# cat /etc/issue.net
```

Run the following command and verify no results are returned:

```
# grep -E -i "(\\v|\\r|\\m|\\s|$(grep '^ID=' /etc/os-release | cut -d= -f2 | sed -e 's/"/\\g'))" /etc/issue.net
```

## Remediation:

Edit the `/etc/issue.net` file with the appropriate contents according to your site policy, remove any instances of `\m`, `\r`, `\s`, `\v` or references to the **OS platform**

*Example:*

```
# echo "Authorized users only. All activity may be monitored and reported." > /etc/issue.net
```

## References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-1, CM-3

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques                          | Tactics | Mitigations |
|------------------------------------------------------|---------|-------------|
| T1018, T1018.000, T1082, T1082.000, T1592, T1592.004 | TA0007  |             |

## 1.7.4 Ensure access to /etc/motd is configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The contents of the `/etc/motd` file are displayed to users after login and function as a message of the day for authenticated users.

### Rationale:

- **IF** - the `/etc/motd` file does not have the correct access configured, it could be modified by unauthorized users with incorrect or misleading information.

### Audit:

Run the following command and verify that if `/etc/motd` exists, **Access** is **644** or more restrictive, **Uid** and **Gid** are both `0/root`:

```
# [ -e /etc/motd ] && stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: { %g/ %G)' /etc/motd

Access: (0644/-rw-r--r--)  Uid: ( 0/ root) Gid: ( 0/ root)
-- OR --
Nothing is returned
```

### Remediation:

Run the following commands to set mode, owner, and group on `/etc/motd`:

```
# chown root:root $(readlink -e /etc/motd)
# chmod u-x,go-wx $(readlink -e /etc/motd)
```

### - OR -

Run the following command to remove the `/etc/motd` file:

```
# rm /etc/motd
```

### References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2



## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1222, T1222.002            | TA0005  | M1022       |

## 1.7.5 Ensure access to /etc/issue is configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The contents of the `/etc/issue` file are displayed to users prior to login for local terminals.

### Rationale:

- **IF** - the `/etc/issue` file does not have the correct access configured, it could be modified by unauthorized users with incorrect or misleading information.

### Audit:

Run the following command and verify **Access** is **644** or more restrictive and **Uid** and **Gid** are both **0/root**:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: { %g/ %G)' /etc/issue
Access: (0644/-rw-r--r--)  Uid: ( 0/ root) Gid: { 0/ root)
```

### Remediation:

Run the following commands to set mode, owner, and group on `/etc/issue`:

```
# chown root:root $(readlink -e /etc/issue)
# chmod u-x,go-wx $(readlink -e /etc/issue)
```

### Default Value:

Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)

### References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1222, T1222.002            | TA0005  | M1022       |

## 1.7.6 Ensure access to /etc/issue.net is configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The contents of the `/etc/issue.net` file are displayed to users prior to login for remote connections from configured services.

### Rationale:

- **IF** - the `/etc/issue.net` file does not have the correct access configured, it could be modified by unauthorized users with incorrect or misleading information.

### Audit:

Run the following command and verify **Access** is **644** or more restrictive and **Uid** and **Gid** are both **0/root**:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U)  Gid: { %g/ %G)' /etc/issue.net
Access: (0644/-rw-r--r--)  Uid: ( 0/ root)   Gid: ( 0/ root)
```

### Remediation:

Run the following commands to set mode, owner, and group on `/etc/issue.net`:

```
# chown root:root $(readlink -e /etc/issue.net)
# chmod u-x,go-wx $(readlink -e /etc/issue.net)
```

### Default Value:

Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)

### References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1222, T1222.002            | TA0005  | M1022       |

### *1.7.7 Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a command line user logon (Manual)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a command line user logon.

#### **Rationale:**

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000228-GPOS-00088

### **Audit:**

Verify the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a command line user logon. Check that the operating system displays a banner at the command line login screen with the following command:

```
# cat /etc/issue
```

If the banner is set correctly, it will return the following text:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

If the banner text does not match the Standard Mandatory DoD Notice and Consent Banner exactly, this is a finding.



## Remediation:

Configure the operating system to display the Standard Mandatory DoD Notice and Consent Banner before granting access to the system via command line logon.

Edit the "/etc/issue" file to replace the default text with the Standard Mandatory DoD Notice and Consent Banner. The DoD-required text is:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only.
```

```
By using this IS (which includes any device attached to this IS), you consent
to the following conditions:
```

```
-The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC
monitoring, network operations and defense, personnel misconduct (PM), law
enforcement (LE), and counterintelligence (CI) investigations.
```

```
-At any time, the USG may inspect and seize data stored on this IS.
```

```
-Communications using, or data stored on, this IS are not private, are
subject to routine monitoring, interception, and search, and may be disclosed
or used for any USG-authorized purpose.
```

```
-This IS includes security measures (e.g., authentication and access
controls) to protect USG interests -- not for your personal benefit or
privacy.
```

```
-Notwithstanding the above, using this IS does not constitute consent to PM,
LE or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or
services by attorneys, psychotherapists, or clergy, and their assistants.
Such communications and work product are private and confidential. See User
Agreement for details."
```

## References:

1. NIST SP 800-53 :: AC-8 a
2. NIST SP 800-53A :: AC-8.1 (ii)

### Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230227  
RULE ID: SV-230227r627750  
STIG ID: RHEL-08-010060  
SEVERITY: CAT II

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

## 1.8 Configure GNOME Display Manager

The GNOME Display Manager (GDM) is a program that manages graphical display servers and handles graphical user logins.

**Note:** If GDM is not installed on the system, this section can be skipped

## 1.8.1 Ensure GNOME Display Manager is removed (Automated)

### Profile Applicability:

- Level 2 - Server

### Description:

The GNOME Display Manager (GDM) is a program that manages graphical display servers and handles graphical user logins.

### Rationale:

If a Graphical User Interface (GUI) is not required, it should be removed to reduce the attack surface of the system.

### Impact:

Removing the GNOME Display manager will remove the Graphical User Interface (GUI) from the system.

### Audit:

Run the following command and verify the output:

```
# rpm -q gdm  
package gdm is not installed
```

### Remediation:

Run the following command to remove the **gdm** package

```
# dnf remove gdm
```

### References:

1. <https://wiki.gnome.org/Projects/GDM>

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1543, T1543.002            | TA0002  |             |

## *1.8.2 Ensure GDM login banner is configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation
- STIG

### **Description:**

GDM is the GNOME Display Manager which handles graphical login for GNOME based systems.

### **Rationale:**

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000228-GPOS-00088

## Audit:

Run the following script to verify that the text banner on the login screen is enabled and set:

```
#!/usr/bin/env bash

{
    l_pkgoutput=""
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package: \"$l_pn\" exists
on the system\n - checking configuration"
    done
    if [ -n "$l_pkgoutput" ]; then
        l_output="" l_output2=""
        echo -e "$l_pkgoutput"
        # Look for existing settings and set variables if they exist
        l_gdmfile="$(grep -Prils '^h*banner-message-enable\b' /etc/dconf/db/*.d)"
        if [ -n "$l_gdmfile" ]; then
            # Set profile name based on dconf db directory ({PROFILE_NAME}.d)
            l_gdmprofile="$(awk -F\ / '{split($NF-1,a,".");print a[1]}' <<< "$l_gdmfile")"
            # Check if banner message is enabled
            if grep -Pisq '^h*banner-message-enable=true\b' "$l_gdmfile"; then
                l_output="$l_output\n - The \"banner-message-enable\" option is enabled in
\"$l_gdmfile\"
"
            else
                l_output2="$l_output2\n - The \"banner-message-enable\" option is not enabled"
            fi
            l_lsbt="$(grep -Pios '^h*banner-message-text=.*$' "$l_gdmfile")"
            if [ -n "$l_lsbt" ]; then
                l_output="$l_output\n - The \"banner-message-text\" option is set in \"$l_gdmfile\"
\n
- banner-message-text is set to:\n - \"$l_lsbt\"
"
            else
                l_output2="$l_output2\n - The \"banner-message-text\" option is not set"
            fi
            if grep -Pq '^h*system-db:$l_gdmprofile' /etc/dconf/profile/"$l_gdmprofile"; then
                l_output="$l_output\n - The \"$l_gdmprofile\" profile exists"
            else
                l_output2="$l_output2\n - The \"$l_gdmprofile\" profile doesn't exist"
            fi
            if [ -f "/etc/dconf/db/$l_gdmprofile" ]; then
                l_output="$l_output\n - The \"$l_gdmprofile\" profile exists in the dconf database"
            else
                l_output2="$l_output2\n - The \"$l_gdmprofile\" profile doesn't exist in the dconf
database"
            fi
            if [ -n "$l_output" ]; then
                l_output2="$l_output2\n - The \"banner-message-enable\" option isn't configured"
            fi
        else
            echo -e "\n\n - GNOME Desktop Manager isn't installed\n - Recommendation is Not
Applicable\n- Audit result:\n *** PASS ***\n"
        fi
        # Report results. If no failures output in l_output2, we pass
        if [ -z "$l_output2" ]; then
            echo -e "\n\n- Audit Result:\n ** PASS **\n$l_output\n"
        else
            echo -e "\n\n- Audit Result:\n ** FAIL **\n - Reason(s) for audit failure:\n$l_output2\n"
            [ -n "$l_output" ] && echo -e "\n\n- Correctly set:\n$l_output\n"
        fi
    fi
}
```

## Remediation:

Run the following script to verify that the banner message is enabled and set:

```
#!/usr/bin/env bash

{
  l_pkgoutput=""
  if command -v dpkg-query > /dev/null 2>&1; then
    l_pq="dpkg-query -W"
  elif command -v rpm > /dev/null 2>&1; then
    l_pq="rpm -q"
  fi
  l_pcl="gdm gdm3" # Space separated list of packages to check
  for l_pn in $l_pcl; do
    $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package: \"$l_pn\" exists
on the system\n - checking configuration"
  done
  if [ -n "$l_pkgoutput" ]; then

    l_gdmprofile="gdm" # Set this to desired profile name IaW Local site policy
    l_bmessage="'Authorized uses only. All activity may be monitored and reported'" # Set to
desired banner message
    if [ ! -f "/etc/dconf/profile/$l_gdmprofile" ]; then
      echo "Creating profile \"$l_gdmprofile\""
      echo -e "user-db:user\nsystem-db:$l_gdmprofile\nfile-
db:/usr/share/$l_gdmprofile/greeter-dconf-defaults" > /etc/dconf/profile/$l_gdmprofile
    fi
    if [ ! -d "/etc/dconf/db/$l_gdmprofile.d/" ]; then
      echo "Creating dconf database directory \"/etc/dconf/db/$l_gdmprofile.d/"
      mkdir /etc/dconf/db/$l_gdmprofile.d/
    fi
    if ! grep -Piq '^h*banner-message-enable|h*=\h*true\b' /etc/dconf/db/$l_gdmprofile.d/*;
then
      echo "creating gdm keyfile for machine-wide settings"
      if ! grep -Piq -- '^h*banner-message-enable|h*=\h*' /etc/dconf/db/$l_gdmprofile.d/*;
then
        l_kfile="/etc/dconf/db/$l_gdmprofile.d/01-banner-message"
        echo -e "\n[org/gnome/login-screen]\nbanner-message-enable=true" >> "$l_kfile"
      else
        l_kfile="$(grep -Pil -- '^h*banner-message-enable|h*=\h*'
/etc/dconf/db/$l_gdmprofile.d/*)"
        ! grep -Pq '^h*\[org/gnome/login-screen\]' "$l_kfile" && sed -ri '/^\s*banner-
message-enable/ i\[org/gnome/login-screen\]' "$l_kfile"
        ! grep -Pq '^h*banner-message-enable|h*=\h*true\b' "$l_kfile" && sed -ri
's/^\s*(banner-message-enable\s*=\s*)(\S+)(\s*.*$)/\1true \3/' "$l_kfile"
        # sed -ri '/^\s*\[org/gnome/login-screen\]/ a\nbanner-message-enable=true'
"$l_kfile"
      fi
    fi
    if ! grep -Piq "^h*banner-message-text=[\`\"']+\\S+" "$l_kfile"; then
      sed -ri "/^\s*banner-message-enable/ a\banner-message-text=$l_bmessage" "$l_kfile"
    fi
    dconf update
  else
    echo -e "\n\n - GNOME Desktop Manager isn't installed\n - Recommendation is Not
Applicable\n - No remediation required\n"
  fi
}
```

## Note:

- There is no character limit for the banner message. gnome-shell autodetects longer stretches of text and enters two column mode.
- The banner message cannot be read from an external file.

**- OR -**



Run the following command to remove the gdm package:

```
# dnf remove gdm
```

### Default Value:

disabled

### References:

1. <https://help.gnome.org/admin/system-admin-guide/stable/login-banner.html.en>
2. NIST SP 800-53 :: AC-8 a
3. NIST SP 800-53A :: AC-8.1 (ii)

### Additional Information:

Additional options and sections may appear in the `/etc/dconf/db/gdm.d/01-banner-message` file.

If a different GUI login service is in use, consult your documentation and apply an equivalent banner.

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-244519  
Rule ID: SV-244519r743806  
STIG ID: RHEL-08-010049  
Severity: CAT II

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
|                             | TA0007  |             |

### *1.8.3 Ensure GDM disable-user-list option is enabled (Automated)*

**Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

**Description:**

GDM is the GNOME Display Manager which handles graphical login for GNOME based systems.

The **disable-user-list** option controls if a list of users is displayed on the login screen

**Rationale:**

Displaying the user list eliminates half of the Userid/Password equation that an unauthorized person would need to log on.

**Audit:**

Run the following script and verify that the **disable-user-list** option is enabled or GNOME isn't installed:

```

#!/usr/bin/env bash

{
    l_pkgoutput=""
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n -
Package: \"$l_pn\" exists on the system\n - checking configuration"
    done
    if [ -n "$l_pkgoutput" ]; then
        output="" output2=""
        l_gdmfile="$(grep -Pril '^\\h*disable-user-list\\h*=\\h*true\\b'
/etc/dconf/db)"
        if [ -n "$l_gdmfile" ]; then
            output="$output\n - The \"disable-user-list\" option is enabled in
\"$l_gdmfile\""
            l_gdmprofile="$(awk -F\\/ '{split($(NF-1),a,\".\");print a[1]}' <<<
"$l_gdmfile")"
            if grep -Pq "\\h*system-db:$l_gdmprofile"
/etc/dconf/profile/"$l_gdmprofile"; then
                output="$output\n - The \"$l_gdmprofile\" exists"
            else
                output2="$output2\n - The \"$l_gdmprofile\" doesn't exist"
            fi
            if [ -f "/etc/dconf/db/$l_gdmprofile" ]; then
                output="$output\n - The \"$l_gdmprofile\" profile exists in the
dconf database"
            else
                output2="$output2\n - The \"$l_gdmprofile\" profile doesn't exist
in the dconf database"
            fi
            else
                output2="$output2\n - The \"disable-user-list\" option is not
enabled"
            fi
            if [ -z "$output2" ]; then
                echo -e "$l_pkgoutput\n- Audit result:\n    *** PASS: ***\n$n$output\n"
            else
                echo -e "$l_pkgoutput\n- Audit Result:\n    *** FAIL:
***\n$n$output2\n"
                [ -n "$output" ] && echo -e "$output\n"
            fi
        else
            echo -e "\n\n - GNOME Desktop Manager isn't installed\n -
Recommendation is Not Applicable\n- Audit result:\n    *** PASS ***\n"
        fi
    }
}

```

## Remediation:

Run the following script to enable the **disable-user-list** option:

**Note:** the **l\_gdm\_profile** variable in the script can be changed if a different profile name is desired in accordance with local site policy.

```
#!/usr/bin/env bash

{
    l_gdmprofile="gdm"
    if [ ! -f "/etc/dconf/profile/$l_gdmprofile" ]; then
        echo "Creating profile \"$l_gdmprofile\""
        echo -e "user-db:user\nsystem-db:$l_gdmprofile\nfile-
db:/usr/share/$l_gdmprofile/greeter-dconf-defaults" >
/etc/dconf/profile/$l_gdmprofile
    fi
    if [ ! -d "/etc/dconf/db/$l_gdmprofile.d/" ]; then
        echo "Creating dconf database directory
\"/etc/dconf/db/$l_gdmprofile.d/\""
        mkdir /etc/dconf/db/$l_gdmprofile.d/
    fi
    if ! grep -Piq '^\\h*disable-user-list\\h*=\\h*true\\b'
/etc/dconf/db/$l_gdmprofile.d/*; then
        echo "creating gdm keyfile for machine-wide settings"
        if ! grep -Piq -- '\\h*\\[org\\/gnome\\/login-screen\\]'
/etc/dconf/db/$l_gdmprofile.d/*; then
            echo -e "\\n[org/gnome/login-screen]\\n# Do not show the user
list\\ndisable-user-list=true" >> /etc/dconf/db/$l_gdmprofile.d/00-login-
screen
        else
            sed -ri '/^\\s*\\[org\\/gnome\\/login-screen\\]/ a\\# Do not show the user
list\\ndisable-user-list=true' $(grep -Pil -- '\\h*\\[org\\/gnome\\/login-
screen\\]' /etc/dconf/db/$l_gdmprofile.d/*)
        fi
    fi
    dconf update
}
```

**Note:** When the user profile is created or changed, the user will need to log out and log in again before the changes will be applied.

**- OR -**

Run the following command to remove the GNOME package:

```
# dnf remove gdm
```

## Default Value:

false

## References:

1. <https://help.gnome.org/admin/system-admin-guide/stable/login-userlist-disable.html.en>

**Additional Information:**

If a different GUI login service is in use and required on the system, consult your documentation to disable displaying the user list

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                                         | Tactics | Mitigations |
|---------------------------------------------------------------------|---------|-------------|
| T1078, T1078.001, T1078.002, T1078.003, T1087, T1087.001, T1087.002 | TA0007  | M1028       |

## 1.8.4 Ensure GDM screen locks when the user is idle (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

### Description:

GNOME Desktop Manager can make the screen lock automatically whenever the user is idle for some amount of time.

- **idle-delay=uint32 {n}** - Number of seconds of inactivity before the screen goes blank
- **lock-delay=uint32 {n}** - Number of seconds after the screen is blank before locking the screen

### Example key file:

```
# Specify the dconf path
[org/gnome/desktop/session]

# Number of seconds of inactivity before the screen goes blank
# Set to 0 seconds if you want to deactivate the screensaver.
idle-delay=uint32 900

# Specify the dconf path
[org/gnome/desktop/screensaver]

# Number of seconds after the screen is blank before locking the screen
lock-delay=uint32 5
```

### Rationale:

Setting a lock-out value reduces the window of opportunity for unauthorized user access to another user's session that has been left unattended.

Satisfies: SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012

### Audit:

Run the following script to verify that the screen locks when the user is idle:

```

#!/usr/bin/env bash

{
    # Check if GNOME Desktop Manager is installed. If package isn't
    installed, recommendation is Not Applicable\n
    # determine system's package manager
    l_pkgoutput=""
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n -
Package: \"$l_pn\" exists on the system\n - checking configuration"
    done
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        l_output="" l_output2=""
        l_idmv="900" # Set for max value for idle-delay in seconds
        l_ldmv="5" # Set for max value for lock-delay in seconds
        # Look for idle-delay to determine profile in use, needed for remaining
        tests
        l_kfile="$(grep -Psril '^\h*idle-delay\h*=\h*uint32\h+\d+\b'
/etc/dconf/db/*)" # Determine file containing idle-delay key
        if [ -n "$l_kfile" ]; then
            # set profile name (This is the name of a dconf database)
            l_profile="$(awk -F '/' '{split($NF-1,a,".");print a[1]}' <<<
"$l_kfile")" #Set the key profile name
            l_pdbdir="/etc/dconf/db/$l_profile.d" # Set the key file dconf db
            directory
            # Confirm that idle-delay exists, includes unit32, and value is
            between 1 and max value for idle-delay
            l_idv="$(awk -F 'uint32' '/idle-delay/{print $2}' "$l_kfile" |
xargs)"
            if [ -n "$l_idv" ]; then
                [ "$l_idv" -gt "0" -a "$l_idv" -le "$l_idmv" ] &&
l_output="$l_output\n - The \"idle-delay\" option is set to \"$l_idv\"
seconds in \"$l_kfile\""
                [ "$l_idv" = "0" ] && l_output2="$l_output2\n - The \"idle-
delay\" option is set to \"$l_idv\" (disabled) in \"$l_kfile\""
                [ "$l_idv" -gt "$l_idmv" ] && l_output2="$l_output2\n - The
\"idle-delay\" option is set to \"$l_idv\" seconds (greater than $l_idmv) in
\"$l_kfile\""
            else
                l_output2="$l_output2\n - The \"idle-delay\" option is not set in
\"$l_kfile\""
            fi
            # Confirm that lock-delay exists, includes unit32, and value is
            between 0 and max value for lock-delay
            l_ldv="$(awk -F 'uint32' '/lock-delay/{print $2}' "$l_kfile" |
xargs)"
            if [ -n "$l_ldv" ]; then
                [ "$l_ldv" -ge "0" -a "$l_ldv" -le "$l_ldmv" ] &&
l_output="$l_output\n - The \"lock-delay\" option is set to \"$l_ldv\"

```

```

seconds in \"$1_kfile\"
    [ \"$1_ldv\" -gt \"$1_ldmv\" ] && l_output2=\"$l_output2\n - The
\\\"lock-delay\\\" option is set to \"$1_ldv\" seconds (greater than $1_ldmv) in
\\\"$1_kfile\\\"
    else
        l_output2=\"$l_output2\n - The \\\"lock-delay\\\" option is not set in
\\\"$1_kfile\\\"
    fi
    # Confirm that dconf profile exists
    if grep -Psq "^\\h*system-db:$1_profile\" /etc/dconf/profile/*; then
        l_output=\"$l_output\n - The \"$1_profile\" profile exists"
    else
        l_output2=\"$l_output2\n - The \"$1_profile\" doesn't exist"
    fi
    # Confirm that dconf profile database file exists
    if [ -f "/etc/dconf/db/$1_profile" ]; then
        l_output=\"$l_output\n - The \"$1_profile\" profile exists in the
dconf database"
    else
        l_output2=\"$l_output2\n - The \"$1_profile\" profile doesn't
exist in the dconf database"
    fi
    else
        l_output2=\"$l_output2\n - The \\\"idle-delay\\\" option doesn't exist,
remaining tests skipped"
    fi
    else
        l_output=\"$l_output\n - GNOME Desktop Manager package is not installed
on the system\n - Recommendation is not applicable"
    fi
    # Report results. If no failures output in l_output2, we pass
    [ -n "$l_pkgoutput" ] && echo -e "\\n$l_pkgoutput"
    if [ -z "$l_output2" ]; then
        echo -e "\\n- Audit Result:\\n  ** PASS **\\n$l_output\\n"
    else
        echo -e "\\n- Audit Result:\\n  ** FAIL **\\n - Reason(s) for audit
failure:\\n$l_output2\\n"
        [ -n "$l_output" ] && echo -e "\\n- Correctly set:\\n$l_output\\n"
    fi
}

```

## Note:

- **idle-delay=uint32** Should be 900 seconds (15 minutes) or less, not 0 (disabled) and follow local site policy
- **lock-delay=uint32** should be 5 seconds or less and follow local site policy



## Remediation:

Create or edit a file in the `/etc/dconf/profile/` and verify it includes the following:

```
user-db:user
system-db:{NAME_OF_DCONF_DATABASE}
```

**Note:** `local` is the name of a dconf database used in the examples.

*Example:*

```
# echo -e '\nuser-db:user\nsystem-db:local' >> /etc/dconf/profile/user
```

Create the directory `/etc/dconf/db/{NAME_OF_DCONF_DATABASE}.d/` if it doesn't already exist:

*Example:*

```
# mkdir /etc/dconf/db/local.d
```

Create the key file `/etc/dconf/db/{NAME_OF_DCONF_DATABASE}.d/{FILE_NAME}` to provide information for the `{NAME_OF_DCONF_DATABASE}` database:

*Example script:*

```
#!/usr/bin/env bash

{
  l_key_file="/etc/dconf/db/local.d/00-screensaver"
  l_idmv="900" # Set max value for idle-delay in seconds (between 1 and 900)
  l_ldmv="5" # Set max value for lock-delay in seconds (between 0 and 5)
  {
    echo '# Specify the dconf path'
    echo '[org/gnome/desktop/session]'
    echo ''
    echo '# Number of seconds of inactivity before the screen goes blank'
    echo '# Set to 0 seconds if you want to deactivate the screensaver.'
    echo "idle-delay=uint32 $l_idmv"
    echo ''
    echo '# Specify the dconf path'
    echo '[org/gnome/desktop/screensaver]'
    echo ''
    echo '# Number of seconds after the screen is blank before locking the screen'
    echo "lock-delay=uint32 $l_ldmv"
  } > "$l_key_file"
}
```

**Note:** You must include the `uint32` along with the integer key values as shown.

Run the following command to update the system databases:

```
# dconf update
```

**Note:** Users must log out and back in again before the system-wide settings take effect.

## References:

1. <https://help.gnome.org/admin/system-admin-guide/stable/desktop-lockscreens.html.en>
2. NIST SP 800-53 Revision 5 :: AC-11 a
3. NIST SP 800-53A :: AC-11.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230352  
Rule ID: SV-230352r646876  
STIG ID: RHEL-08-020060  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                       | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u></b><br>Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. |  |  |  |
| v7               | <b>16.11 <u>Lock Workstation Sessions After Inactivity</u></b><br>Automatically lock workstation sessions after a standard period of inactivity.                                                                                                                                                                              |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1461                       | TA0027  |             |

## 1.8.5 Ensure GDM screen locks cannot be overridden (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

### Description:

GNOME Desktop Manager can make the screen lock automatically whenever the user is idle for some amount of time.

By using the lockdown mode in dconf, you can prevent users from changing specific settings.

To lock down a dconf key or subpath, create a locks subdirectory in the keyfile directory. The files inside this directory contain a list of keys or subpaths to lock. Just as with the keyfiles, you may add any number of files to this directory.

### Example Lock File:

```
# Lock desktop screensaver settings
/org/gnome/desktop/session/idle-delay
/org/gnome/desktop/screensaver/lock-delay
```

### Rationale:

Setting a lock-out value reduces the window of opportunity for unauthorized user access to another user's session that has been left unattended.

Without locking down the system settings, user settings take precedence over the system settings.

Satisfies: SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012, SRG-OS-000480-GPOS-00227

### Audit:

Run the following script to verify that the screen lock cannot be overridden:

```

#!/usr/bin/env bash

{
    # Check if GNOME Desktop Manager is installed. If package isn't installed, recommendation is
    Not Applicable\n
    # determine system's package manager
    l_pkgoutput=""
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n - Package: \"$l_pn\" exists
on the system\n - checking configuration"
    done
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        l_output="" l_output2=""
        # Look for idle-delay to determine profile in use, needed for remaining tests
        l_kfd="/etc/dconf/db/$(grep -Psrl '^h*idle-delayh*=\h*uint32\h+\d+\b' /etc/dconf/db/* |
awk -F'/' '{split($(NF-1),a,".");print a[1]}').d" #set directory of key file to be locked
        l_kfd2="/etc/dconf/db/$(grep -Psrl '^h*lock-delayh*=\h*uint32\h+\d+\b' /etc/dconf/db/* |
| awk -F'/' '{split($(NF-1),a,".");print a[1]}').d" #set directory of key file to be locked
        if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options can't be locked
            if grep -Prilq '\org/gnome/desktop/session/idle-delay\b' "$l_kfd"; then
                l_output="$l_output\n - \"idle-delay\" is locked in \"$(grep -Pril
'\org/gnome/desktop/session/idle-delay\b' "$l_kfd")\"
            else
                l_output2="$l_output2\n - \"idle-delay\" is not locked"
            fi
        else
            l_output2="$l_output2\n - \"idle-delay\" is not set so it can not be locked"
        fi
        if [ -d "$l_kfd2" ]; then # If key file directory doesn't exist, options can't be locked
            if grep -Prilq '\org/gnome/desktop/screensaver/lock-delay\b' "$l_kfd2"; then
                l_output="$l_output\n - \"lock-delay\" is locked in \"$(grep -Pril
'\org/gnome/desktop/screensaver/lock-delay\b' "$l_kfd2")\"
            else
                l_output2="$l_output2\n - \"lock-delay\" is not locked"
            fi
        else
            l_output2="$l_output2\n - \"lock-delay\" is not set so it can not be locked"
        fi
    else
        l_output="$l_output\n - GNOME Desktop Manager package is not installed on the system\n -
Recommendation is not applicable"
    fi
    # Report results. If no failures output in l_output2, we pass
    [ -n "$l_pkgoutput" ] && echo -e "\n$l_pkgoutput"
    if [ -z "$l_output2" ]; then
        echo -e "\n- Audit Result:\n ** PASS **\n$l_output\n"
    else
        echo -e "\n- Audit Result:\n ** FAIL **\n - Reason(s) for audit failure:\n$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
    fi
}

```

## Remediation:

Run the following script to ensure screen locks cannot be overridden:

```

#!/usr/bin/env bash

{
    # Check if GNOME Desktop Manager is installed. If package isn't
    installed, recommendation is Not Applicable\n
    # determine system's package manager
    l_pkgoutput=""
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="y" && echo -e "\n -
Package: \"$l_pn\" exists on the system\n - remediating configuration if
needed"
    done
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        # Look for idle-delay to determine profile in use, needed for remaining
        tests
        l_kfd="/etc/dconf/db/$(grep -Psril '^h*idle-
delay\h*=\h*uint32\h+\d+\b' /etc/dconf/db/* | awk -F'/' '{split($(NF-
1),a,".");print a[1]}').d" #set directory of key file to be locked
        # Look for lock-delay to determine profile in use, needed for remaining
        tests
        l_kfd2="/etc/dconf/db/$(grep -Psril '^h*lock-
delay\h*=\h*uint32\h+\d+\b' /etc/dconf/db/* | awk -F'/' '{split($(NF-
1),a,".");print a[1]}').d" #set directory of key file to be locked
        if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options
        can't be locked
            if grep -Prilq '^h*\s*/org/gnome/desktop/session/idle-delay\b'
"$l_kfd"; then
                echo " - \"idle-delay\" is locked in \"$(grep -Pril
'^h*\s*/org/gnome/desktop/session/idle-delay\b' "$l_kfd")\"
            else
                echo "creating entry to lock \"idle-delay\"
                [ ! -d "$l_kfd/locks" ] && echo "creating directory $l_kfd/locks"
                && mkdir "$l_kfd/locks"
                {
                    echo -e '\n# Lock desktop screensaver idle-delay setting'
                    echo '/org/gnome/desktop/session/idle-delay'
                } >> "$l_kfd/locks/00-screensaver
            fi
        else
            echo -e " - \"idle-delay\" is not set so it can not be locked\n -
Please follow Recommendation \"Ensure GDM screen locks when the user is
idle\" and follow this Recommendation again"
        fi
        if [ -d "$l_kfd2" ]; then # If key file directory doesn't exist,
        options can't be locked
            if grep -Prilq '^h*\s*/org/gnome/desktop/screensaver/lock-
delay\b' "$l_kfd2"; then
                echo " - \"lock-delay\" is locked in \"$(grep -Pril
'^h*\s*/org/gnome/desktop/screensaver/lock-delay\b' "$l_kfd2")\"

```

```

        else
            echo "creating entry to lock \"lock-delay\""
            [ ! -d "$l_kfd2"/locks ] && echo "creating directory
$l_kfd2/locks" && mkdir "$l_kfd2"/locks
            {
                echo -e '\n# Lock desktop screensaver lock-delay setting'
                echo '/org/gnome/desktop/screensaver/lock-delay'
            } >> "$l_kfd2"/locks/00-screensaver
        fi
    else
        echo -e " - \"lock-delay\" is not set so it can not be locked\n -
Please follow Recommendation \"Ensure GDM screen locks when the user is
idle\" and follow this Recommendation again"
    fi
    else
        echo -e " - GNOME Desktop Manager package is not installed on the
system\n - Recommendation is not applicable"
    fi
}

```

Run the following command to update the system databases:

```
# dconf update
```

**Note:** Users must log out and back in again before the system-wide settings take effect.

#### References:

1. <https://help.gnome.org/admin/system-admin-guide/stable/desktop-lockscreens.html.en>
2. <https://help.gnome.org/admin/system-admin-guide/stable/dconf-lockdown.html.en>
3. IST SP 800-53 Revision 4 :: AC-11 a NIST SP 800-53 Revision 5 :: AC-11 a
4. NIST SP 800-53A :: AC-11.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230354  
Rule ID: SV-230354r743990  
STIG ID: RHEL-08-020080  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                       | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u></b><br>Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. |  |  |  |
| v7               | <b>16.11 <u>Lock Workstation Sessions After Inactivity</u></b><br>Automatically lock workstation sessions after a standard period of inactivity.                                                                                                                                                                              |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1456                       | TA0027  |             |

### *1.8.6 Ensure GDM automatic mounting of removable media is disabled (Automated)*

**Profile Applicability:**

- Level 1 - Server
- Level 2 - Workstation

**Description:**

By default GNOME automatically mounts removable media when inserted as a convenience to the user.

**Rationale:**

With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.

**Impact:**

The use of portable hard drives is very common for workstation users. If your organization allows the use of portable storage or media on workstations and physical access controls to workstations is considered adequate there is little value add in turning off automounting.

**Audit:**

Run the following script to verify automatic mounting is disabled:



```

#!/usr/bin/env bash

{
    l_pkgoutput="" l_output="" l_output2=""
    # Check if GNOME Desktop Manager is installed. If package isn't
    installed, recommendation is Not Applicable\n
    # determine system's package manager
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n -
Package: \"$l_pn\" exists on the system\n - checking configuration"
    done
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        echo -e "$l_pkgoutput"
        # Look for existing settings and set variables if they exist
        l_kfile="$(grep -Prils -- '^\\h*automount\\b' /etc/dconf/db/*.d)"
        l_kfile2="$(grep -Prils -- '^\\h*automount-open\\b' /etc/dconf/db/*.d)"
        # Set profile name based on dconf db directory ({PROFILE_NAME}.d)
        if [ -f "$l_kfile" ]; then
            l_gpname="$(awk -F\\ / '{split($(NF-1),a,".");print a[1]}' <<<
"$l_kfile")"
        elif [ -f "$l_kfile2" ]; then
            l_gpname="$(awk -F\\ / '{split($(NF-1),a,".");print a[1]}' <<<
"$l_kfile2")"
        fi
        # If the profile name exist, continue checks
        if [ -n "$l_gpname" ]; then
            l_gpdir="/etc/dconf/db/$l_gpname.d"
            # Check if profile file exists
            if grep -Pq -- "^\\h*system-db:$l_gpname\\b" /etc/dconf/profile/*;
then
                l_output="$l_output\n - dconf database profile file \"$(grep -Pl
-- "^\\h*system-db:$l_gpname\\b" /etc/dconf/profile/*)\" exists"
            else
                l_output2="$l_output2\n - dconf database profile isn't set"
            fi
            # Check if the dconf database file exists
            if [ -f "/etc/dconf/db/$l_gpname" ]; then
                l_output="$l_output\n - The dconf database \"$l_gpname\" exists"
            else
                l_output2="$l_output2\n - The dconf database \"$l_gpname\"
doesn't exist"
            fi
            # check if the dconf database directory exists
            if [ -d "$l_gpdir" ]; then
                l_output="$l_output\n - The dconf directory \"$l_gpdir\" existst"
            else
                l_output2="$l_output2\n - The dconf directory \"$l_gpdir\"
doesn't exist"
            fi
        fi
    fi
}

```

```

        # check automount setting
        if grep -Pqrs -- '^\\h*automount\\h*=\\h*false\\b' "$l_kfile"; then
            l_output="$l_output\\n - \\\"automount\\\" is set to false in:
\\\"$l_kfile\\\"\"
        else
            l_output2="$l_output2\\n - \\\"automount\\\" is not set correctly\"
        fi
        # check automount-open setting
        if grep -Pqs -- '^\\h*automount-open\\h*=\\h*false\\b' "$l_kfile2"; then
            l_output="$l_output\\n - \\\"automount-open\\\" is set to false in:
\\\"$l_kfile2\\\"\"
        else
            l_output2="$l_output2\\n - \\\"automount-open\\\" is not set
correctly\"
        fi
        else
            # Setings don't exist. Nothing further to check
            l_output2="$l_output2\\n - neither \\\"automount\\\" or \\\"automount-
open\\\" is set\"
        fi
        else
            l_output="$l_output\\n - GNOME Desktop Manager package is not installed
on the system\\n - Recommendation is not applicable\"
        fi
        # Report results. If no failures output in l_output2, we pass
        if [ -z \"$l_output2\" ]; then
            echo -e \"\\n- Audit Result:\\n  ** PASS **\\n$l_output\\n\"
        else
            echo -e \"\\n- Audit Result:\\n  ** FAIL **\\n - Reason(s) for audit
failure:\\n$l_output2\\n\"
            [ -n \"$l_output\" ] && echo -e \"\\n- Correctly set:\\n$l_output\\n\"
        fi
    }
}

```

## Remediation:

Run the following script to disable automatic mounting of media for all GNOME users:

```

#!/usr/bin/env bash

{
    l_pkgoutput=""
    l_gpname="local" # Set to desired dconf profile name (default is local)
    # Check if GNOME Desktop Manager is installed. If package isn't
    installed, recommendation is Not Applicable\n
    # determine system's package manager
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n -
Package: \"$l_pn\" exists on the system\n - checking configuration"
    done
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        echo -e "$l_pkgoutput"
        # Look for existing settings and set variables if they exist
        l_kfile="$(grep -Prils -- '^h*automount\b' /etc/dconf/db/*.d)"
        l_kfile2="$(grep -Prils -- '^h*automount-open\b' /etc/dconf/db/*.d)"
        # Set profile name based on dconf db directory ({PROFILE_NAME}.d)
        if [ -f "$l_kfile" ]; then
            l_gpname="$(awk -F\ / '{split($(NF-1),a,".");print a[1]}' <<<
"$l_kfile")"
            echo " - updating dconf profile name to \"$l_gpname\""
        elif [ -f "$l_kfile2" ]; then
            l_gpname="$(awk -F\ / '{split($(NF-1),a,".");print a[1]}' <<<
"$l_kfile2")"
            echo " - updating dconf profile name to \"$l_gpname\""
        fi
        # check for consistency (Clean up configuration if needed)
        if [ -f "$l_kfile" ] && [ "$(awk -F\ / '{split($(NF-1),a,".");print
a[1]}' <<< "$l_kfile")" != "$l_gpname" ]; then
            sed -ri "/^s*automount\s*=/s/^/# /" "$l_kfile"
            l_kfile="/etc/dconf/db/$l_gpname.d/00-media-automount"
        fi
        if [ -f "$l_kfile2" ] && [ "$(awk -F\ / '{split($(NF-1),a,".");print
a[1]}' <<< "$l_kfile2")" != "$l_gpname" ]; then
            sed -ri "/^s*automount-open\s*=/s/^/# /" "$l_kfile2"
        fi
        [ -z "$l_kfile" ] && l_kfile="/etc/dconf/db/$l_gpname.d/00-media-
automount"
        # Check if profile file exists
        if grep -Pq -- "^h*system-db:$l_gpname\b" /etc/dconf/profile/*; then
            echo -e "\n - dconf database profile exists in: \"$(grep -Pl --
"^h*system-db:$l_gpname\b" /etc/dconf/profile/*)\""
        else
            if [ ! -f "/etc/dconf/profile/user" ]; then
                l_gpfile="/etc/dconf/profile/user"
            else
                l_gpfile="/etc/dconf/profile/user2"
            fi
        fi
    fi
}

```

```

        echo -e " - creating dconf database profile"
        {
            echo -e "\nuser-db:user"
            echo "system-db:$l_gpname"
        } >> "$l_gpfile"
    fi
    # create dconf directory if it doesn't exists
    l_gpdir="/etc/dconf/db/$l_gpname.d"
    if [ -d "$l_gpdir" ]; then
        echo " - The dconf database directory \"$l_gpdir\" exists"
    else
        echo " - creating dconf database directory \"$l_gpdir\""
        mkdir "$l_gpdir"
    fi
    # check automount-open setting
    if grep -Pqs -- '^\h*automount-open\h*=\h*false\b' "$l_kfile"; then
        echo " - \"automount-open\" is set to false in: \"$l_kfile\""
    else
        echo " - creating \"automount-open\" entry in \"$l_kfile\""
        ! grep -Psq -- '^\h*\[org\/gnome\/desktop\/media-handling\]\b'
"$l_kfile" && echo '[org/gnome/desktop/media-handling]' >> "$l_kfile"
        sed -ri '/^\s*\[org\/gnome\/desktop\/media-handling\]/a
\nautomount-open=false' "$l_kfile"
    fi
    # check automount setting
    if grep -Pqs -- '^\h*automount\h*=\h*false\b' "$l_kfile"; then
        echo " - \"automount\" is set to false in: \"$l_kfile\""
    else
        echo " - creating \"automount\" entry in \"$l_kfile\""
        ! grep -Psq -- '^\h*\[org\/gnome\/desktop\/media-handling\]\b'
"$l_kfile" && echo '[org/gnome/desktop/media-handling]' >> "$l_kfile"
        sed -ri '/^\s*\[org\/gnome\/desktop\/media-handling\]/a
\nautomount=false' "$l_kfile"
    fi
    # update dconf database
    dconf update
else
    echo -e "\n - GNOME Desktop Manager package is not installed on the
system\n - Recommendation is not applicable"
fi
}

```

## - OR -

Run the following command to uninstall the GNOME desktop Manager package:

```
# dnf remove gdm
```

## References:

1. <https://access.redhat.com/solutions/20107>

**CIS Controls:**

| Controls Version | Control                                                                                                                                      | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <u>10.3 Disable Autorun and Autoplay for Removable Media</u><br>Disable autorun and autoplay auto-execute functionality for removable media. |  |  |  |
| v7               | <u>8.5 Configure Devices Not To Auto-run Content</u><br>Configure devices to not auto-run content from removable media.                      |  |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics        | Mitigations |
|-----------------------------|----------------|-------------|
| T1091, T1091.000            | TA0001, TA0008 | M1042       |

## *1.8.7 Ensure GDM disabling automatic mounting of removable media is not overridden (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 2 - Workstation

### **Description:**

By default GNOME automatically mounts removable media when inserted as a convenience to the user

By using the lockdown mode in dconf, you can prevent users from changing specific settings.

To lock down a dconf key or subpath, create a locks subdirectory in the keyfile directory. The files inside this directory contain a list of keys or subpaths to lock. Just as with the keyfiles, you may add any number of files to this directory.

### *Example Lock File:*

```
# Lock automount settings
/org/gnome/desktop/media-handling/automount
/org/gnome/desktop/media-handling/automount-open
```

### **Rationale:**

With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.

### **Impact:**

The use of portable hard drives is very common for workstation users

### **Audit:**

Run the following script to verify disable automatic mounting is locked:

```

#!/usr/bin/env bash

{
    # Check if GNOME Desktop Manager is installed. If package isn't
    installed, recommendation is Not Applicable\n
    # determine system's package manager
    l_pkgoutput=""
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n -
Package: \"$l_pn\" exists on the system\n - checking configuration"
    done
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        l_output="" l_output2=""
        echo -e "$l_pkgoutput\n"
        # Look for idle-delay to determine profile in use, needed for remaining
        tests
        l_kfd="/etc/dconf/db/$(grep -Psril '^h*automount\b' /etc/dconf/db/* |
awk -F'/' '{split($(NF-1),a,".");print a[1]}').d" #set directory of key file
to be locked
        l_kfd2="/etc/dconf/db/$(grep -Psril '^h*automount-open\b'
/etc/dconf/db/* | awk -F'/' '{split($(NF-1),a,".");print a[1]}').d" #set
directory of key file to be locked
        if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options
        can't be locked
            if grep -Priq '^h*\org/gnome/desktop/media-
handling\automount\b' "$l_kfd"; then
                l_output="$l_output\n - \"automount\" is locked in \"$(grep -Pri
l '^h*\org/gnome/desktop/media-handling\automount\b' "$l_kfd")\"
            else
                l_output2="$l_output2\n - \"automount\" is not locked"
            fi
        else
            l_output2="$l_output2\n - \"automount\" is not set so it can not be
        locked"
        fi
        if [ -d "$l_kfd2" ]; then # If key file directory doesn't exist,
        options can't be locked
            if grep -Priq '^h*\org/gnome/desktop/media-handling\automount-
open\b' "$l_kfd2"; then
                l_output="$l_output\n - \"automount-open\" is locked in \"$(grep
        -Pri
l '^h*\org/gnome/desktop/media-handling\automount-open\b'
        \"$l_kfd2\")\"
            else
                l_output2="$l_output2\n - \"automount-open\" is not locked"
            fi
        else
            l_output2="$l_output2\n - \"automount-open\" is not set so it can
        not be locked"
        fi
    fi
}

```

```
    else
        l_output="$l_output\n - GNOME Desktop Manager package is not installed
on the system\n - Recommendation is not applicable"
    fi
    # Report results. If no failures output in l_output2, we pass
    if [ -z "$l_output2" ]; then
        echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
    else
        echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
    fi
}
```

### **Remediation:**

Run the following script to lock/disable automatic mounting of media for all GNOME users:



```

#!/usr/bin/env bash

{
    # Check if GNOME Desktop Manager is installed. If package isn't
    installed, recommendation is Not Applicable\n
    # determine system's package manager
    l_pkgoutput=""
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="y" && echo -e "\n -
Package: \"$l_pn\" exists on the system\n - remediating configuration if
needed"
    done
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        # Look for automount to determine profile in use, needed for remaining
        tests
        l_kfd="/etc/dconf/db/$(grep -Psril '^h*automount\b' /etc/dconf/db/*/ |
awk -F'/' '{split($(NF-1),a,".");print a[1]})'.d" #set directory of key file
to be locked
        # Look for automount-open to determine profile in use, needed for
        remaining tests
        l_kfd2="/etc/dconf/db/$(grep -Psril '^h*automount-open\b'
/etc/dconf/db/*/ | awk -F'/' '{split($(NF-1),a,".");print a[1]})'.d" #set
directory of key file to be locked
        if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options
        can't be locked
            if grep -Priq '^h*\org/gnome/desktop/media-
handling/automount\b' "$l_kfd"; then
                echo " - \"automount\" is locked in \"$(grep -Pril
'^h*\org/gnome/desktop/media-handling/automount\b' "$l_kfd")\"
            else
                echo " - creating entry to lock \"automount\"
                [ ! -d "$l_kfd/locks" ] && echo "creating directory $l_kfd/locks"
&& mkdir "$l_kfd/locks"
                {
                    echo -e '\n# Lock desktop media-handling automount setting'
                    echo '/org/gnome/desktop/media-handling/automount'
                } >> "$l_kfd/locks/00-media-automount
            fi
        else
            echo -e " - \"automount\" is not set so it can not be locked\n -
Please follow Recommendation \"Ensure GDM automatic mounting of removable
media is disabled\" and follow this Recommendation again"
        fi
        if [ -d "$l_kfd2" ]; then # If key file directory doesn't exist,
        options can't be locked
            if grep -Priq '^h*\org/gnome/desktop/media-handling/automount-
open\b' "$l_kfd2"; then
                echo " - \"automount-open\" is locked in \"$(grep -Pril
'^h*\org/gnome/desktop/media-handling/automount-open\b' "$l_kfd2")\"

```

```

else
    echo " - creating entry to lock \"automount-open\""
    [ ! -d "$1_kfd2"/locks ] && echo "creating directory
$1_kfd2/locks" && mkdir "$1_kfd2"/locks
    {
        echo -e '\n# Lock desktop media-handling automount-open
setting'
        echo '/org/gnome/desktop/media-handling/automount-open'
    } >> "$1_kfd2"/locks/00-media-automount
    fi
else
    echo -e " - \"automount-open\" is not set so it can not be locked\n
- Please follow Recommendation \"Ensure GDM automatic mounting of removable
media is disabled\" and follow this Recommendation again"
    fi
    # update dconf database
    dconf update
else
    echo -e " - GNOME Desktop Manager package is not installed on the
system\n - Recommendation is not applicable"
    fi
}

```

## References:

1. <https://help.gnome.org/admin/system-admin-guide/stable/dconf-lockdown.html.en>

## CIS Controls:

| Controls Version | Control                                                                                                                                      | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | 10.3 <u>Disable Autorun and Autoplay for Removable Media</u><br>Disable autorun and autoplay auto-execute functionality for removable media. |  |  |  |
| v7               | 8.5 <u>Configure Devices Not To Auto-run Content</u><br>Configure devices to not auto-run content from removable media.                      |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics        | Mitigations |
|-----------------------------|----------------|-------------|
| T1091, T1091.000            | TA0001, TA0008 | M1042       |

### *1.8.8 Ensure the operating system does not allow an unattended or automatic logon to the system via a graphical user interface (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Unattended or automatic logon via the operating system's graphical user interface must not be allowed.

#### **Rationale:**

Failure to restrict system access to authenticated users negatively impacts operating system security.

#### **Audit:**

Verify the operating system does not allow an unattended or automatic logon to the system via a graphical user interface.

Note: This requirement assumes the use of the RHEL 8 default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Check for the value of the "AutomaticLoginEnable" in the "/etc/gdm/custom.conf" file with the following command:

```
# grep -i automaticloginenable /etc/gdm/custom.conf
AutomaticLoginEnable=false
```

If the value of "AutomaticLoginEnable" is not set to "false", this is a finding.

Remediation:

Configure the operating system to not allow an unattended or automatic logon to the system via a graphical user interface.  
Add or edit the line for the "AutomaticLoginEnable" parameter in the [daemon] section of the "/etc/gdm/custom.conf" file to "false":

```
[daemon]
AutomaticLoginEnable=false
```

Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024  
  
GROUP ID: V-230329  
RULE ID: SV-230329r877377  
STIG ID: RHEL-08-010820  
SEVERITY: CAT I

CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                       |  |  |

### *1.8.9 Ensure GDM autorun-never is enabled (Automated)*

**Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

**Description:**

The **autorun-never** setting allows the GNOME Desktop Display Manager to disable autorun through GDM.

**Rationale:**

Malware on removable media may take advantage of Autorun features when the media is inserted into a system and execute.

**Audit:**

Run the following script to verify that **autorun-never** is set to **true** for GDM:

```

#!/usr/bin/env bash

{
    l_pkgoutput="" l_output="" l_output2=""
    # Check if GNOME Desktop Manager is installed. If package isn't
installed, recommendation is Not Applicable\n
    # determine system's package manager
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n -
Package: \"$l_pn\" exists on the system\n - checking configuration"
        echo -e "$l_pkgoutput"
    done
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        echo -e "$l_pkgoutput"
        # Look for existing settings and set variables if they exist
        l_kfile="$(grep -Prils -- '^\\h*autorun-never\\b' /etc/dconf/db/*.d)"
        # Set profile name based on dconf db directory ({PROFILE_NAME}.d)
        if [ -f "$l_kfile" ]; then
            l_gpname="$(awk -F\\ / '{split($(NF-1),a,".");print a[1]}' <<<
"$l_kfile")"
        fi
        # If the profile name exist, continue checks
        if [ -n "$l_gpname" ]; then
            l_gpdir="/etc/dconf/db/$l_gpname.d"
            # Check if profile file exists
            if grep -Pq -- "^\\h*system-db:$l_gpname\\b" /etc/dconf/profile/*;
then
                l_output="$l_output\n - dconf database profile file \"$(grep -Pl
-- "^\\h*system-db:$l_gpname\\b" /etc/dconf/profile/*)\" exists"
            else
                l_output2="$l_output2\n - dconf database profile isn't set"
            fi
            # Check if the dconf database file exists
            if [ -f "/etc/dconf/db/$l_gpname" ]; then
                l_output="$l_output\n - The dconf database \"$l_gpname\" exists"
            else
                l_output2="$l_output2\n - The dconf database \"$l_gpname\"
doesn't exist"
            fi
            # check if the dconf database directory exists
            if [ -d "$l_gpdir" ]; then
                l_output="$l_output\n - The dconf directory \"$l_gpdir\" existst"
            else
                l_output2="$l_output2\n - The dconf directory \"$l_gpdir\"
doesn't exist"
            fi
            # check autorun-never setting
            if grep -Pqrs -- '^\\h*autorun-never\\h*=\\h*true\\b' "$l_kfile"; then
                l_output="$l_output\n - \"autorun-never\" is set to true in:

```

```

\"$l_kfile\"
    else
        l_output2=\"$l_output2\n - \"autorun-never\" is not set correctly"
    fi
else
    # Settings don't exist. Nothing further to check
    l_output2=\"$l_output2\n - \"autorun-never\" is not set"
fi
else
    l_output=\"$l_output\n - GNOME Desktop Manager package is not installed
on the system\n - Recommendation is not applicable"
fi
# Report results. If no failures output in l_output2, we pass
if [ -z "$l_output2" ]; then
    echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
else
    echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
    [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
fi
}

```

## Remediation:

Run the following script to set **autorun-never** to **true** for GDM users:

```

#!/usr/bin/env bash

{
    l_pkgoutput="" l_output="" l_output2=""
    l_gpname="local" # Set to desired dconf profile name (default is local)
    # Check if GNOME Desktop Manager is installed. If package isn't
    installed, recommendation is Not Applicable\n
    # determine system's package manager
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n -
Package: \"$l_pn\" exists on the system\n - checking configuration"
    done
    echo -e "$l_pkgoutput"
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        echo -e "$l_pkgoutput"
        # Look for existing settings and set variables if they exist
        l_kfile="$(grep -Prils -- '^h*autorun-never\b' /etc/dconf/db/*.d)"
        # Set profile name based on dconf db directory ({PROFILE_NAME}.d)
        if [ -f "$l_kfile" ]; then
            l_gpname="$(awk -F/ '{split($(NF-1),a,".");print a[1]}' <<<
"$l_kfile")"
            echo " - updating dconf profile name to \"$l_gpname\""
        fi
        [ ! -f "$l_kfile" ] && l_kfile="/etc/dconf/db/$l_gpname.d/00-media-
autorun"
        # Check if profile file exists
        if grep -Pq -- "^h*system-db:$l_gpname\b" /etc/dconf/profile/*; then
            echo -e "\n - dconf database profile exists in: \"$(grep -Pl --
"^h*system-db:$l_gpname\b" /etc/dconf/profile/*)\n"
        else
            [ ! -f "/etc/dconf/profile/user" ] &&
l_gpfile="/etc/dconf/profile/user" || l_gpfile="/etc/dconf/profile/user2"
            echo -e " - creating dconf database profile"
            {
                echo -e "\nuser-db:user"
                echo "system-db:$l_gpname"
            } >> "$l_gpfile"
        fi
        # create dconf directory if it doesn't exists
        l_gpdir="/etc/dconf/db/$l_gpname.d"
        if [ -d "$l_gpdir" ]; then
            echo " - The dconf database directory \"$l_gpdir\" exists"
        else
            echo " - creating dconf database directory \"$l_gpdir\""
            mkdir "$l_gpdir"
        fi
        # check autorun-never setting
        if grep -Pqs -- '^h*autorun-never\b*=\b*true\b' "$l_kfile"; then
            echo " - \"autorun-never\" is set to true in: \"$l_kfile\""
        fi
    fi
}

```



```

else
    echo " - creating or updating \"autorun-never\" entry in
\"$1_kfile\"
    if grep -Psq -- '^\\h*autorun-never' "$1_kfile"; then
        sed -ri 's/(^\\s*autorun-never\\s*=\\s*)(\\S+)(\\s*.*)$/\\1true \\3/'
"$1_kfile"
    else
        ! grep -Psq -- '^\\h*\\[org\\/gnome\\/desktop\\/media-handling\\]\\b'
"$1_kfile" && echo '[org/gnome/desktop/media-handling]' >> "$1_kfile"
        sed -ri '/^\\s*\\[org\\/gnome\\/desktop\\/media-handling\\]/a
\\nautorun-never=true' "$1_kfile"
    fi
fi
else
    echo -e "\n - GNOME Desktop Manager package is not installed on the
system\n - Recommendation is not applicable"
fi
# update dconf database
dconf update
}

```

#### Default Value:

false

#### CIS Controls:

| Controls Version | Control                                                                                                                                      | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | 10.3 <u>Disable Autorun and Autoplay for Removable Media</u><br>Disable autorun and autoplay auto-execute functionality for removable media. |  |  |  |
| v7               | 8.5 <u>Configure Devices Not To Auto-run Content</u><br>Configure devices to not auto-run content from removable media.                      |  |  |  |

#### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1091                       |         |             |

### *1.8.10 Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed when using a graphical user interface (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The x86 Ctrl-Alt-Delete key sequence must be disabled if a graphical user interface is installed.

#### **Rationale:**

A locally logged-on user, who presses Ctrl-Alt-Delete, when at the console, can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot. In a graphical user environment, risk of unintentional reboot from the Ctrl-Alt-Delete sequence is reduced because the user will be prompted before any action is taken.

#### **Audit:**

Verify the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed when using a graphical user interface with the following command:  
This requirement assumes the use of the default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

```
# grep logout /etc/dconf/db/local.d/*  
logout=''
```

If the "logout" key is bound to an action, is commented out, or is missing, this is a finding.

## Remediation:

Configure the system to disable the Ctrl-Alt-Delete sequence when using a graphical user interface by creating or editing the `/etc/dconf/db/local.d/00-disable-CAD` file.  
Add the setting to disable the Ctrl-Alt-Delete sequence for a graphical user interface:

```
[org/gnome/settings-daemon/plugins/media-keys]
logout=''
```

Note: The value above is set to two single quotations.  
Then update the dconf settings:

```
# dconf update
```

## References:

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230530  
Rule ID: SV-230530r646883  
STIG ID: RHEL-08-040171  
Severity: CAT I

## CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### 1.8.11 Ensure GDM autorun-never is not overridden (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The autorun-never setting allows the GNOME Desktop Display Manager to disable autorun through GDM.

By using the lockdown mode in dconf, you can prevent users from changing specific settings.

To lock down a dconf key or subpath, create a locks subdirectory in the keyfile directory. The files inside this directory contain a list of keys or subpaths to lock. Just as with the keyfiles, you may add any number of files to this directory.

Example Lock File:

```
# Lock desktop media-handling settings
/org/gnome/desktop/media-handling/autorun-never
```

#### Rationale:

Malware on removable media may take advantage of Autorun features when the media is inserted into a system and execute.

#### Audit:

Run the following script to verify that **autorun-never=true** cannot be overridden:

```
#!/usr/bin/env bash

{
    # Check if GNOME Desktop Manager is installed. If package isn't
    installed, recommendation is Not Applicable\n
    # determine system's package manager
    l_pkgoutput=""
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="$l_pkgoutput\n -
Package: \"$l_pn\" exists on the system\n - checking configuration"
    done
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        l_output="" l_output2=""
        echo -e "$l_pkgoutput\n"
        # Look for idle-delay to determine profile in use, needed for remaining
        tests
        l_kfd="/etc/dconf/db/$(grep -Psril '^h*autorun-never\b'
/etc/dconf/db/* | awk -F '/' '{split($(NF-1),a,".");print a[1]}').d" #set
directory of key file to be locked
        if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options
        can't be locked
            if grep -Priq '^h*\org/gnome/desktop/media-handling/autorun-
never\b' "$l_kfd"; then
                l_output="$l_output\n - \"autorun-never\" is locked in \"$(grep -
Priil '^h*\org/gnome/desktop/media-handling/autorun-never\b' "$l_kfd")\"
            else
                l_output2="$l_output2\n - \"autorun-never\" is not locked"
            fi
        else
            l_output2="$l_output2\n - \"autorun-never\" is not set so it can not
be locked"
        fi
    else
        l_output="$l_output\n - GNOME Desktop Manager package is not installed
on the system\n - Recommendation is not applicable"
    fi
    # Report results. If no failures output in l_output2, we pass
    if [ -z "$l_output2" ]; then
        echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
    else
        echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
    fi
}

```

**Remediation:**

Run the following script to ensure that `autorun-never=true` cannot be overridden:

```
#!/usr/bin/env bash

{
    # Check if GNOME Desktop Manager is installed. If package isn't
    installed, recommendation is Not Applicable\n
    # determine system's package manager
    l_pkgoutput=""
    if command -v dpkg-query > /dev/null 2>&1; then
        l_pq="dpkg-query -W"
    elif command -v rpm > /dev/null 2>&1; then
        l_pq="rpm -q"
    fi
    # Check if GDM is installed
    l_pcl="gdm gdm3" # Space separated list of packages to check
    for l_pn in $l_pcl; do
        $l_pq "$l_pn" > /dev/null 2>&1 && l_pkgoutput="y" && echo -e "\n -
Package: \"$l_pn\" exists on the system\n - remediating configuration if
needed"
    done
    # Check configuration (If applicable)
    if [ -n "$l_pkgoutput" ]; then
        # Look for autorun to determine profile in use, needed for remaining
        tests
        l_kfd="/etc/dconf/db/$(grep -Psril '^h*autorun-never\b'
/etc/dconf/db/* | awk -F '/' '{split($(NF-1),a,".");print a[1]}').d" #set
directory of key file to be locked
        if [ -d "$l_kfd" ]; then # If key file directory doesn't exist, options
        can't be locked
            if grep -Priq '^h*\ /org/gnome\ /desktop\ /media-handling\ /autorun-
never\b' "$l_kfd"; then
                echo " - \"autorun-never\" is locked in \"$(grep -Pril
'^h*\ /org/gnome\ /desktop\ /media-handling\ /autorun-never\b' "$l_kfd")\""
            else
                echo " - creating entry to lock \"autorun-never\""
                [ ! -d "$l_kfd"/locks ] && echo "creating directory $l_kfd/locks"
                && mkdir "$l_kfd"/locks
                {
                    echo -e '\n# Lock desktop media-handling autorun-never
setting'
                    echo '/org/gnome/desktop/media-handling/autorun-never'
                } >> "$l_kfd"/locks/00-media-autorun
            fi
        else
            echo -e " - \"autorun-never\" is not set so it can not be locked\n -
Please follow Recommendation \"Ensure GDM autorun-never is enabled\" and
follow this Recommendation again"
        fi
        # update dconf database
        dconf update
    else
        echo -e " - GNOME Desktop Manager package is not installed on the
system\n - Recommendation is not applicable"
    fi
}
}
```

**CIS Controls:**

| Controls Version | Control                                                                                                                                      | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <u>10.3 Disable Autorun and Autoplay for Removable Media</u><br>Disable autorun and autoplay auto-execute functionality for removable media. |  |  |  |
| v7               | <u>8.5 Configure Devices Not To Auto-run Content</u><br>Configure devices to not auto-run content from removable media.                      |  |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics        | Mitigations |
|-----------------------------|----------------|-------------|
| T1091                       | TA0001, TA0008 |             |



### *1.8.12 Ensure the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must initiate a session lock for graphical user interfaces when the screensaver is activated.

#### **Rationale:**

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Satisfies: SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012, SRG-OS-000480-GPOS-00227

#### **Audit:**

Verify the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated with the following command:

Note: This requirement assumes the use of the default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

```
# gsettings get org.gnome.desktop.screensaver lock-delay
uint32 5
```

If the "uint32" setting is missing, or is not set to "5" or less, this is a finding.

Remediation:

Configure the operating system to initiate a session lock for graphical user interfaces when a screensaver is activated.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

Note: The example below is using the database "local" for the system, so if the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
# touch /etc/dconf/db/local.d/00-screensaver

[org/gnome/desktop/screensaver]
lock-delay=uint32 5
```

The "uint32" must be included along with the integer key values as shown. Update the system databases:

```
# dconf update
```

References:

- 1. NIST SP 800-53 :: AC-11 a
- 2. NIST SP 800-53A :: AC-11.1 (ii)

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244535

Rule ID: SV-244535r743854

STIG ID: RHEL-08-020031

Severity: CAT II

CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                | IG 1        | IG 2        | IG 3        |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-------------|-------------|
| v8               | <b>4.3 Configure Automatic Session Locking on Enterprise Assets</b><br>Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. | <div></div> | <div></div> | <div></div> |
| v7               | <b>16.11 Lock Workstation Sessions After Inactivity</b><br>Automatically lock workstation sessions after a standard period of inactivity.                                                                                                                                                                              | <div></div> | <div></div> | <div></div> |

### 1.8.13 Ensure XDMCP is not enabled (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

X Display Manager Control Protocol (XDMCP) is designed to provide authenticated access to display management services for remote displays

#### Rationale:

XDMCP is inherently insecure.

- XDMCP is not a ciphered protocol. This may allow an attacker to capture keystrokes entered by a user
- XDMCP is vulnerable to man-in-the-middle attacks. This may allow an attacker to steal the credentials of legitimate users by impersonating the XDMCP server.

#### Audit:

Run the following command and verify the output:

```
# grep -Eis '^s*Enable\s*=\s*true' /etc/gdm/custom.conf  
Nothing should be returned
```

#### Remediation:

Edit the file `/etc/gdm/custom.conf` and remove the line:

```
Enable=true
```

#### Default Value:

false (This is denoted by no `Enabled=` entry in the file `/etc/gdm/custom.conf` in the `[xdmcp]` section)

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                          | Tactics | Mitigations |
|------------------------------------------------------|---------|-------------|
| T1040, T1040.000, T1056, T1056.001, T1557, T1557.000 | TA0002  | M1050       |

### *1.8.14 Ensure the operating system disables the user logon list for graphical user interfaces (Automated)*

**Profile Applicability:**

- STIG

**Description:**

The operating system must disable the user list at logon for graphical user interfaces.

**Rationale:**

Leaving the user list enabled is a security risk since it allows anyone with physical access to the system to enumerate known user accounts without authenticated access to the system.

**Audit:**

Verify the operating system disables the user logon list for graphical user interfaces with the following command:

Note: This requirement assumes the use of the default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

```
# gsettings get org.gnome.login-screen disable-user-list
true
```

If the setting is "false", this is a finding.

## Remediation:

Configure the operating system to disable the user list at logon for graphical user interfaces.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

**Note:** The example below is using the database "gdm" for the system, so if the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
#!/usr/bin/env bash

{
    if ! grep -P -- '^h*\[org/gnome/login-screen\]\h*$', then
        printf '\n%s' "[org/gnome/login-screen]" "disable-user-list=true" >>
/etc/dconf/db/gdm.d/00-login-screen
    else
        printf '\n%s\n' "disable-user-list=true" >> /etc/dconf/db/gdm.d/00-
login-screen
    fi
}
```

Update the system databases:

```
# dconf update
```

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244536  
Rule ID: SV-244536r743857  
STIG ID: RHEL-08-020032  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 <u>Use Unique Passwords</u></b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 <u>Use Unique Passwords</u></b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

### *1.8.15 Ensure GDM login banner displays the Mandatory DoD Notice and Consent Banner (Manual)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Banners are used to warn connecting users of the particular site's policy regarding connection

#### **Rationale:**

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:



You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

I've read & consent to terms in IS user agreem't.

**Note:** This Recommendation only applies to systems with the GNOME Desktop manager package installed

## Audit:

**Note:** If the system does not have a graphical user interface installed, this Recommendation is Not Applicable.

Run the following command to verify the operating system displays the exact approved Standard Mandatory DoD Notice and Consent Banner text:

```
# grep -Psi -- '^\\h*banner-message-text\\b' /etc/dconf/db/local.d/*
```

Output should read:

```
banner-message-text="You are accessing a U.S. Government \ (USG\ ) Information
System \ (IS\ ) that is provided for USG-authorized use only.\s+By using this
IS \ (which includes any device attached to this IS\ ), you consent to the
following conditions:\s+-The USG routinely intercepts and monitors
communications on this IS for purposes including, but not limited to,
penetration testing, COMSEC monitoring, network operations and defense,
personnel misconduct \ (PM\ ), law enforcement \ (LE\ ), and counterintelligence
\ (CI\ ) investigations.\s+-At any time, the USG may inspect and seize data
stored on this IS.\s+-Communications using, or data stored on, this IS are
not private, are subject to routine monitoring, interception, and search, and
may be disclosed or used for any USG-authorized purpose.\s+-This IS includes
security measures \ (e.g., authentication and access controls\ ) to protect USG
interests--not for your personal benefit or privacy.\s+-Notwithstanding the
above, using this IS does not constitute consent to PM, LE or CI
investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or
services by attorneys, psychotherapists, or clergy, and their assistants.
Such communications and work product are private and confidential. See User
Agreement for details."
```

Verify the **banner-message-text=** option exists, is not commented out, and includes the Standard Mandatory DoD Notice and Consent Banner exactly.

## Remediation:

Edit the `/etc/gdm3/greeter.dconf-defaults` file.

Edit the file `/etc/dconf/db/local.d/01-banner-message` and add or modify the `banner-message-text` parameter in the `[org/gnome/login-screen]` section as follows:

```
banner-message-text='You are accessing a U.S. Government (USG) Information
System (IS) that is provided for USG-authorized use only.\n\nBy using this IS
(which includes any device attached to this IS), you consent to the following
conditions:\n\n-The USG routinely intercepts and monitors communications on
this IS for purposes including, but not limited to, penetration testing,
COMSEC monitoring, network operations and defense, personnel misconduct (PM),
law enforcement (LE), and counterintelligence (CI) investigations.\n\n-At any
time, the USG may inspect and seize data stored on this IS.\n\n-
Communications using, or data stored on, this IS are not private, are subject
to routine monitoring, interception, and search, and may be disclosed or used
for any USG-authorized purpose.\n\n-This IS includes security measures (e.g.,
authentication and access controls) to protect USG interests--not for your
personal benefit or privacy.\n\n-Notwithstanding the above, using this IS
does not constitute consent to PM, LE or CI investigative searching or
monitoring of the content of privileged communications, or work product,
related to personal representation or services by attorneys,
psychotherapists, or clergy, and their assistants. Such communications and
work product are private and confidential. See User Agreement for details.'
```

**Note:** the `\n` characters are for formatting only and will not be displayed on the graphical interface.

Run the following commands to update the GDM with the new configuration:

```
# dconf update
# systemctl reload-or-restart gdm
```

## References:

1. NIST SP 800-53 :: AC-8 a
2. NIST SP 800-53A :: AC-8.1 (ii)

## Additional Information:

### Red Hat Enterprise Linux 8

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024  
  
GROUP ID: V-230226  
RULE ID: SV-230226r743916  
STIG ID: RHEL-08-010050  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### *1.8.16 Ensure the operating system prevents users from overriding the session idle-delay setting for the graphical user interface (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must prevent a user from overriding the session idle-delay setting for the graphical user interface.

#### **Rationale:**

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Implementing session settings will have little value if a user is able to manipulate these settings from the defaults prescribed in the other requirements of this implementation guide.

Locking these settings from non-privileged users is crucial to maintaining a protected baseline.

Satisfies: SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012, SRG-OS-000480-GPOS-00227

## Audit:

Verify, the operating system prevents a user from overriding settings for graphical user interfaces.

Note: This requirement assumes the use of the default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Determine which profile the system database is using with the following command:

```
# grep system-db /etc/dconf/profile/user  
  
system-db:local
```

Check that graphical settings are locked from non-privileged user modification with the following command:

Note: The example below is using the database "local" for the system, so the path is "/etc/dconf/db/local.d". This path must be modified if a database other than "local" is being used.

```
# grep -i idle /etc/dconf/db/local.d/locks/*  
  
/org/gnome/desktop/session/idle-delay
```

If the command does not return at least the example result, this is a finding.

## Remediation:

Configure the operating system to prevent a user from overriding settings for graphical user interfaces.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

Note: The example below is using the database "local" for the system, so if the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
# touch /etc/dconf/db/local.d/locks/session
```

Add the following setting to prevent non-privileged users from modifying it:

```
/org/gnome/desktop/session/idle-delay
```

## References:

1. NIST SP 800-53 :: AC-11 a
2. NIST SP 800-53A :: AC-11.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244538  
Rule ID: SV-244538r743863  
STIG ID: RHEL-08-020081  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                       | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u></b><br>Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. |  |  |  |
| v7               | <b>16.11 <u>Lock Workstation Sessions After Inactivity</u></b><br>Automatically lock workstation sessions after a standard period of inactivity.                                                                                                                                                                              |  |  |  |

### *1.8.17 Ensure the operating system prevents users from overriding the screensaver lock-enabled setting for the graphical user interface (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must prevent a user from overriding the screensaver lock-enabled setting for the graphical user interface.

#### **Rationale:**

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Implementing session settings will have little value if a user is able to manipulate these settings from the defaults prescribed in the other requirements of this implementation guide.

Locking these settings from non-privileged users is crucial to maintaining a protected baseline.

Satisfies: SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012, SRG-OS-000480-GPOS-00227



## Audit:

Verify, the operating system prevents a user from overriding settings for graphical user interfaces.

Note: This requirement assumes the use of the default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

Determine which profile the system database is using with the following command:

```
# grep system-db /etc/dconf/profile/user  
  
system-db:local
```

Check that graphical settings are locked from non-privileged user modification with the following command:

Note: The example below is using the database "local" for the system, so the path is "/etc/dconf/db/local.d". This path must be modified if a database other than "local" is being used.

```
# grep -i lock-enabled /etc/dconf/db/local.d/locks/*  
  
/org/gnome/desktop/screensaver/lock-enabled
```

If the command does not return at least the example result, this is a finding.

## Remediation:

Configure the operating system to prevent a user from overriding settings for graphical user interfaces.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

Note: The example below is using the database "local" for the system, so if the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
# touch /etc/dconf/db/local.d/locks/session
```

Add the following setting to prevent non-privileged users from modifying it:

```
/org/gnome/desktop/screensaver/lock-enabled
```

## References:

1. NIST SP 800-53 :: AC-11 a
2. NIST SP 800-53A :: AC-11.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244539  
Rule ID: SV-244539r743866  
STIG ID: RHEL-08-020082  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                       | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u></b><br>Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. |  |  |  |
| v7               | <b>16.11 <u>Lock Workstation Sessions After Inactivity</u></b><br>Automatically lock workstation sessions after a standard period of inactivity.                                                                                                                                                                              |  |  |  |

### *1.8.18 Ensure the operating system initiates a session lock for all connection types using smartcard when the smartcard is removed (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### **Description:**

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

#### **Rationale:**

The session lock is implemented at the point where session activity can be determined. Rather than be forced to wait for a period of time to expire before the user session can be locked, RHEL 8 needs to provide users with the ability to manually invoke a session lock so users can secure their session if it is necessary to temporarily vacate the immediate physical vicinity.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

#### **Audit:**

Run the following command to verify the operating system enables a user's session lock until that user re-establishes access using established identification and authentication procedures:

```
# grep -R removal-action /etc/dconf/db/*  
  
/etc/dconf/db/distro.d/20-authselect:removal-action='lock-screen'
```

## Remediation:

Configure the operating system to enable a user's session lock until that user re-establishes access using established identification and authentication procedures. Select/Create an authselect profile and incorporate the "with-smartcard-lock-on-removal" feature with the following example:

```
# authselect select sssd with-smartcard with-smartcard-lock-on-removal
```

### - OR -

Alternatively, the dconf settings can be edited in the `/etc/dconf/db/*` location:

Edit or add the `[org/gnome/settings-daemon/peripherals/smartcard]` section of the database file and add or update the following lines:

`removal-action='lock-screen'`

Update the system databases:

```
# dconf update
```

## References:

1. NIST SP 800-53 Revision 5 :: AC-11 b
2. NIST SP 800-53A :: AC-11.1 (iii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230351  
Rule ID: SV-230351r792899  
STIG ID: RHEL-08-020050  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                      | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.1 <u>Establish and Maintain a Secure Configuration Process</u></b><br>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |

### *1.8.19 Ensure the operating system enables a user's session lock until that user re-establishes access (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures for graphical user sessions.

#### **Rationale:**

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

Regardless of where the session lock is determined and implemented, once invoked, the session lock must remain in place until the user reauthenticates. No other activity aside from reauthentication must unlock the system.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

#### **Audit:**

Verify the operating system enables a user's session lock until that user re-establishes access using established identification and authentication procedures with the following command:

```
# gsettings get org.gnome.desktop.screensaver lock-enabled  
  
true
```

If the setting is "false", this is a finding.

Note: This requirement assumes the use of the default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

## Remediation:

Configure the operating system to enable a user's session lock until that user re-establishes access using established identification and authentication procedures. Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following example:

```
# vi /etc/dconf/db/local.d/00-screensaver
```

Edit the "[org/gnome/desktop/screensaver]" section of the database file and add or update the following lines:

```
# Set this to true to lock the screen when the screensaver activates
lock-enabled=true
```

Update the system databases:

```
# dconf update
```

## References:

1. NIST SP 800-53 Revision 5 :: AC-11 b
2. NIST SP 800-53A :: AC-11.1 (iii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230347  
Rule ID: SV-230347r627750  
STIG ID: RHEL-08-020030  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.1 Establish and Maintain a Secure Configuration Process</b><br>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |
| v7               | <b>16.11 Lock Workstation Sessions After Inactivity</b><br>Automatically lock workstation sessions after a standard period of inactivity.                                                                                                                                                                                                                                                                             |  |  |  |

## 1.9 Ensure the "tmux" package installed (Automated)

### Profile Applicability:

- STIG

### Description:

The operating system must have the tmux package installed.

### Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. Rather than be forced to wait for a period of time to expire before the user session can be locked, the operating system needs to provide users with the ability to manually invoke a session lock so users can secure their session if it is necessary to temporarily vacate the immediate physical vicinity.

Tmux is a terminal multiplexer that enables a number of terminals to be created, accessed, and controlled from a single screen. Red Hat endorses tmux as the recommended session controlling package.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

### Audit:

Verify the operating system has the "tmux" package installed, by running the following command:

```
# dnf list installed tmux  
  
tmux.x86_64 2.7-1.el8 @repository
```

If "tmux" is not installed, this is a finding.

### Remediation:

Configure the operating system to enable a user to initiate a session lock via tmux. Install the "tmux" package, if it is not already installed, by running the following command:

```
# dnf install tmux
```

### References:

1. NIST SP 800-53 :: AC-11 b
2. NIST SP 800-53A :: AC-11.1 (iii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244537  
Rule ID: SV-244537r743860  
STIG ID: RHEL-08-020039  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u></b><br>Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.                                                                                                                                                                                         |    |    |    |
| v8               | <b>4.10 <u>Enforce Automatic Device Lockout on Portable End-User Devices</u></b><br>Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts. |                                                                                       |   |   |
| v7               | <b>16.11 <u>Lock Workstation Sessions After Inactivity</u></b><br>Automatically lock workstation sessions after a standard period of inactivity.                                                                                                                                                                                                                                                                                                                                                                      |  |  |  |



## *1.10 Ensure the system has the packages required to enable the hardware random number generator entropy gatherer service (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system must have the packages required to use the hardware random number generator entropy gatherer service.

### **Rationale:**

The most important characteristic of a random number generator is its randomness, namely its ability to deliver random numbers that are impossible to predict. Entropy in computer security is associated with the unpredictability of a source of randomness. The random source with high entropy tends to achieve a uniform distribution of random values. Random number generators are one of the most important building blocks of cryptosystems.

The rngd service feeds random data from hardware device to kernel random device. Quality (non-predictable) random number generation is important for several security functions (i.e., ciphers).

### **Audit:**

Check that the operating system has the packages required to enable the hardware random number generator entropy gatherer service with the following command:

```
# dnf list installed rng-tools  
  
rng-tools.x86_64 6.8-3.el8 @anaconda
```

If the "rng-tools" package is not installed, this is a finding.

### **Remediation:**

Install the packages required to enable the hardware random number generator entropy gatherer service with the following command:

```
# dnf install rng-tools
```

### **References:**

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244527  
Rule ID: SV-244527r743830  
STIG ID: RHEL-08-010472  
Severity: CAT III

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

## 1.11 Ensure the mailx package is installed (Automated)

### Profile Applicability:

- STIG

### Description:

The operating system must be configured to allow sending email notifications of unauthorized configuration changes to designated personnel.

### Rationale:

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating system's IMO/ISSO and SAs must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

### Audit:

Run the following command to verify that the **mailx** package is installed on the system:

```
# dnf list installed mailx  
mailx.x86_64      12.5-29.el8      @rhel-8-for-x86_64-baseos-rpm
```

**Note:** The **mailx** package provides the **mail** command that is used to send email messages.

### Remediation:

Run the following command to install the **mailx** package on the system:

```
# dnf install mailx
```

### References:

1. NIST SP 800-53 Revision 5 :: CM-3 (5)

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-256974  
Rule ID: SV-256974r902755  
STIG ID: RHEL-08-010358  
Severity: CAT II

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

## 1.12 Ensure the operating system accepts PIV credentials (Automated)

### Profile Applicability:

- STIG

### Description:

The operating system must accept Personal Identity Verification (PIV) credentials.

### Rationale:

The use of PIV credentials facilitates standardization and reduces the risk of unauthorized access.

The DoD has mandated the use of the Common Access Card (CAC) to support identity management and personal authentication for systems covered under Homeland Security Presidential Directive (HSPD) 12, as well as making the CAC a primary component of layered protection for national security systems.

### Audit:

Verify the operating system accepts PIV credentials.

Check that the "opensc" package is installed on the system with the following command:

```
# dnf list installed opensc  
  
opensc.x86_64 0.19.0-5.el8 @anaconda
```

Check that "opensc" accepts PIV cards with the following command:

```
# opensc-tool --list-drivers | grep -i piv  
  
PIV-II Personal Identity Verification Card
```

If the "opensc" package is not installed and the "opensc-tool" driver list does not include "PIV-II", this is a finding.

### Remediation:

Configure the operating system to accept PIV credentials.  
Install the "opensc" package using the following command:

```
# dnf install opensc
```

### References:

1. NIST SP 800-53 Revision 5 :: IA-2 (12)

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230275  
Rule ID: SV-230275r854030  
STIG ID: RHEL-08-010410  
Severity: CAT II

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

## *1.13 Ensure the operating system has the packages required for multifactor authentication (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system must have the packages required for multifactor authentication installed.

### **Rationale:**

Using an authentication device, such as a DoD Common Access Card (CAC) or token that is separate from the information system, ensures that even if the information system is compromised, credentials stored on the authentication device will not be affected.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification (PIV) card and the DoD CAC.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

### **Audit:**

Verify the operating system has the packages required for multifactor authentication installed with the following commands:

```
# dnf list installed openssl-pkcs11  
  
openssl-pkcs11.x86_64 0.4.8-2.el8 @anaconda
```

If the "openssl-pkcs11" package is not installed, ask the administrator to indicate what type of multifactor authentication is being utilized and what packages are installed to support it. If there is no evidence of multifactor authentication being used, this is a finding.

## Remediation:

Configure the operating system to implement multifactor authentication by installing the required package with the following command:

```
# dnf install openssl-pkcs11
```

## References:

1. NIST SP 800-53 Revision 4 :: IA-2 (11)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230273  
Rule ID: SV-230273r854028  
STIG ID: RHEL-08-010390  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>6.3 <u>Require MFA for Externally-Exposed Applications</u></b><br>Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard. |      | ●    | ●    |
| v8               | <b>6.5 <u>Require MFA for Administrative Access</u></b><br>Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.                                                                      | ●    | ●    | ●    |
| v7               | <b>16.3 <u>Require Multi-factor Authentication</u></b><br>Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.                                                                                                 |      | ●    | ●    |



## 2 Services

While applying system updates and patches helps correct known vulnerabilities, one of the best ways to protect the system against as yet unreported vulnerabilities is to disable all services that are not required for normal system operation. This prevents the exploitation of vulnerabilities discovered at a later date. If a service is not enabled, it cannot be exploited. The actions in this section of the document provide guidance on some services which can be safely disabled and under which circumstances, greatly reducing the number of possible threats to the resulting system. Additionally, some services which should remain enabled but with secure configuration are covered as well as insecure service clients.

## 2.1 Configure Server Services

This section describes services that are installed on systems that specifically need to run these services. If any of these services are not required, it is recommended that the package be removed.

- **IF** - the package is required for a dependency:

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy
- Stop and mask the service and/or socket to reduce the potential attack surface

The following commands can be used to stop and mask the service and socket:

```
# systemctl stop <service_name>.socket <service_name>.service  
# systemctl mask <service_name>.socket <service_name>.service
```

**Note:** This should not be considered a comprehensive list of services not required for normal system operation. You may wish to consider additions to those listed here for your environment

## 2.1.1 Ensure autofs services are not in use (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation
- STIG

### Description:

**autofs** allows automatic mounting of devices, typically including CD/DVDs and USB drives.

### Rationale:

With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.

### Impact:

The use of portable hard drives is very common for workstation users. If your organization allows the use of portable storage or media on workstations and physical access controls to workstations is considered adequate there is little value add in turning off automounting.

There may be packages that are dependent on the **autofs** package. If the **autofs** package is removed, these dependent packages will be removed as well. Before removing the **autofs** package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the **autofs.service** leaving the **autofs** package installed.

## Audit:

As a preference **autofs** should not be installed unless other packages depend on it. Run the following command to verify **autofs** is not installed:

```
# rpm -q autofs  
package autofs is not installed
```

- OR -

- IF - the package is required for dependencies:

Run the following command to verify **autofs.service** is not enabled:

```
# systemctl is-enabled autofs.service 2>/dev/null | grep 'enabled'  
Nothing should be returned
```

Run the following command to verify the **autofs.service** is not active:

```
# systemctl is-active autofs.service 2>/dev/null | grep '^active'  
Nothing should be returned
```

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop **autofs.service** and remove **autofs** package:

```
# systemctl stop autofs.service  
# dnf remove autofs
```

- OR -

- IF - the **autofs** package is required as a dependency:

Run the following commands to stop and mask **autofs.service**:

```
# systemctl stop autofs.service  
# systemctl mask autofs.service
```

## References:

1. NIST SP 800-53 Rev. 5: SI-3, MP-7
2. NIST SP 800-53 Revision 5 :: IA-3
3. NIST SP 800-53A :: IA-3.1 (ii)

## Additional Information:

This control should align with the tolerance of the use of portable drives and optical media in the organization. On a server requiring an admin to manually mount media can be part of defense-in-depth to reduce the risk of unapproved software or information being introduced or proprietary software or information being exfiltrated. If admins commonly use flash drives and Server access has sufficient physical controls, requiring manual mounting may not increase security.

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230502  
Rule ID: SV-230502r627750  
STIG ID: RHEL-08-040070  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                      | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <u>10.3 Disable Autorun and Autoplay for Removable Media</u><br>Disable autorun and autoplay auto-execute functionality for removable media. |   |   |   |
| v7               | <u>8.5 Configure Devices Not To Auto-run Content</u><br>Configure devices to not auto-run content from removable media.                      |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques                                            | Tactics | Mitigations |
|------------------------------------------------------------------------|---------|-------------|
| T1068, T1068.000, T1203, T1203.000, T1211, T1211.000, T1212, T1212.000 |         |             |

## 2.1.2 Ensure avahi daemon services are not in use (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

### Description:

Avahi is a free zeroconf implementation, including a system for multicast DNS/DNS-SD service discovery. Avahi allows programs to publish and discover services and hosts running on a local network with no specific configuration. For example, a user can plug a computer into a network and Avahi automatically finds printers to print to, files to look at and people to talk to, as well as network services running on the machine.

### Rationale:

Automatic discovery of network services is not normally required for system functionality. It is recommended to remove this package to reduce the potential attack surface.

### Impact:

There may be packages that are dependent on the **avahi** package. If the **avahi** package is removed, these dependent packages will be removed as well. Before removing the **avahi** package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the **avahi-daemon.socket** and **avahi-daemon.service** leaving the **avahi** package installed.

## Audit:

Run the following command to verify the **avahi** package is not installed:

```
# rpm -q avahi  
  
package avahi is not installed
```

**- OR -**

**- IF -** the **avahi** package is required as a dependency:

Run the following command to verify **avahi-daemon.socket** and **avahi-daemon.service** are not enabled:

```
# systemctl is-enabled avahi-daemon.socket avahi-daemon.service 2>/dev/null |  
grep 'enabled'  
  
Nothing should be returned
```

Run the following command to verify **avahi-daemon.socket** and **avahi-daemon.service** are not active:

```
# systemctl is-active avahi-daemon.socket avahi-daemon.service 2>/dev/null |  
grep '^active'  
  
Nothing should be returned
```

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop **avahi-daemon.socket** and **avahi-daemon.service**, and remove the **avahi** package:

```
# systemctl stop avahi-daemon.socket avahi-daemon.service  
# dnf remove avahi
```

**- OR -**

**- IF -** the **avahi** package is required as a dependency:

Run the following commands to stop and mask the **avahi-daemon.socket** and **avahi-daemon.service**:

```
# systemctl stop avahi-daemon.socket avahi-daemon.service  
# systemctl mask avahi-daemon.socket avahi-daemon.service
```

## References:

1. NIST SP 800-53 Rev. 5: SI-4

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                          | Tactics | Mitigations |
|------------------------------------------------------|---------|-------------|
| T1203, T1203.000, T1210, T1210.000, T1543, T1543.002 | TA0008  | M1042       |



### 2.1.3 Ensure dhcp server services are not in use (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The Dynamic Host Configuration Protocol (DHCP) is a service that allows machines to be dynamically assigned IP addresses. There are two versions of the DHCP protocol **DHCPv4** and **DHCPv6**. At startup the server may be started for one or the other via the **-4** or **-6** arguments.

#### Rationale:

Unless a system is specifically set up to act as a DHCP server, it is recommended that the **dhcp-server** package be removed to reduce the potential attack surface.

#### Impact:

There may be packages that are dependent on the **dhcp-server** package. If the **dhcp-server** package is removed, these dependent packages will be removed as well. Before removing the **dhcp-server** package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the **dhcpcd.service** and **dhcpcd6.service** leaving the **dhcp-server** package installed.

## Audit:

Run the following command to verify **dhcp-server** is not installed:

```
# rpm -q dhcp-server  
  
package dhcp-server is not installed
```

**- OR -**

**- IF -** the package is required for dependencies:

Run the following command to verify **dhcpcd.service** and **dhcpcd6.service** are not enabled:

```
# systemctl is-enabled dhcpcd.service dhcpcd6.service 2>/dev/null | grep  
'enabled'  
  
Nothing should be returned
```

Run the following command to verify **dhcpcd.service** and **dhcpcd6.service** are not active:

```
# systemctl is-active dhcpcd.service dhcpcd6.service 2>/dev/null | grep  
'^active'  
  
Nothing should be returned
```

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop **dhcpcd.service** and **dhcpcd6.service** and remove **dhcp-server** package:

```
# systemctl stop dhcpcd.service dhcpcd6.service  
# dnf remove dhcp-server
```

**- OR -**

**- IF -** the **dhcp-server** package is required as a dependency:

Run the following commands to stop and mask **dhcpcd.service** and **dhcpcd6.service**:

```
# systemctl stop dhcpcd.service dhcpcd6.service  
# systemctl mask dhcpcd.service dhcpcd6.service
```

## References:

1. dhcpcd(8)
2. NIST SP 800-53 Rev. 5: CM-7

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                          | Tactics | Mitigations |
|------------------------------------------------------|---------|-------------|
| T1203, T1203.000, T1210, T1210.000, T1543, T1543.002 | TA0008  | M1042       |

## *2.1.4 Ensure dns server services are not in use (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The Domain Name System (DNS) is a hierarchical naming system that maps names to IP addresses for computers, services and other resources connected to a network.

### **Rationale:**

Unless a system is specifically designated to act as a DNS server, it is recommended that the package be removed to reduce the potential attack surface.

### **Impact:**

There may be packages that are dependent on the `bind` package. If the `bind` package is removed, these dependent packages will be removed as well. Before removing the `bind` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the `named.service` leaving the `bind` package installed.

## Audit:

Run one of the following commands to verify **bind** is not installed:

```
# rpm -q bind  
  
package bind is not installed
```

- OR -

- IF - the package is required for dependencies:

Run the following command to verify **named.service** is not enabled:

```
# systemctl is-enabled named.service 2>/dev/null | grep 'enabled'  
  
Nothing should be returned
```

Run the following command to verify the **named.service** is not active:

```
# systemctl is-active named.service 2>/dev/null | grep '^active'  
  
Nothing should be returned
```

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop **named.service** and remove **bind** package:

```
# systemctl stop named.service  
# dnf remove bind
```

- OR -

- IF - the **bind** package is required as a dependency:

Run the following commands to stop and mask **named.service**:

```
# systemctl stop named.service  
# systemctl mask named.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      | ●    | ●    |
| v7               | <u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      | ●    | ●    |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                          | Tactics | Mitigations |
|------------------------------------------------------|---------|-------------|
| T1203, T1203.000, T1210, T1210.000, T1543, T1543.002 | TA0008  | M1042       |

## 2.1.5 Ensure dnsmasq services are not in use (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

**dnsmasq** is a lightweight tool that provides DNS caching, DNS forwarding and DHCP (Dynamic Host Configuration Protocol) services.

### Rationale:

Unless a system is specifically designated to act as a DNS caching, DNS forwarding and/or DHCP server, it is recommended that the package be removed to reduce the potential attack surface.

### Impact:

There may be packages that are dependent on the **dnsmasq** package. If the **dnsmasq** package is removed, these dependent packages will be removed as well. Before removing the **dnsmasq** package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the **dnsmasq.service** leaving the **dnsmasq** package installed.

## Audit:

Run one of the following commands to verify **dnsmasq** is not installed:

```
# rpm -q dnsmasq  
  
package dnsmasq is not installed
```

- OR -

- IF - the package is required for dependencies:

Run the following command to verify **dnsmasq.service** is not enabled:

```
# systemctl is-enabled dnsmasq.service 2>/dev/null | grep 'enabled'  
  
Nothing should be returned
```

Run the following command to verify the **dnsmasq.service** is not active:

```
# systemctl is-active dnsmasq.service 2>/dev/null | grep '^active'  
  
Nothing should be returned
```

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop **dnsmasq.service** and remove **dnsmasq** package:

```
# systemctl stop dnsmasq.service  
# dnf remove dnsmasq
```

- OR -

- IF - the **dnsmasq** package is required as a dependency:

Run the following commands to stop and mask the **dnsmasq.service**:

```
# systemctl stop dnsmasq.service  
# systemctl mask dnsmasq.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7



**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                          | Tactics | Mitigations |
|------------------------------------------------------|---------|-------------|
| T1203, T1203.000, T1210, T1210.000, T1543, T1543.002 | TA0008  | M1042       |

## *2.1.6 Ensure ftp server services are not in use (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation
- STIG

### **Description:**

FTP (File Transfer Protocol) is a traditional and widely used standard tool for transferring files between a server and clients over a network, especially where no authentication is necessary (permits anonymous users to connect to a server).

### **Rationale:**

Unless there is a need to run the system as a FTP server, it is recommended that the package be removed to reduce the potential attack surface.

### **Impact:**

There may be packages that are dependent on the `vsftpd` package. If the `vsftpd` package is removed, these dependent packages will be removed as well. Before removing the `vsftpd` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the `vsftpd.service` leaving the `vsftpd` package installed.

## Audit:

Run the following command to verify **vsftpd** is not installed:

```
# rpm -q vsftpd  
  
package vsftpd is not installed
```

- OR -

- IF - the package is required for dependencies:

Run the following command to verify **vsftpd** service is not enabled:

```
# systemctl is-enabled vsftpd.service 2>/dev/null | grep 'enabled'  
  
Nothing should be returned
```

Run the following command to verify the **vsftpd** service is not active:

```
# systemctl is-active vsftpd.service 2>/dev/null | grep '^active'  
  
Nothing should be returned
```

## Note:

- Other ftp server packages may exist. They should also be audited, if not required and authorized by local site policy
- If the package is required for a dependency:
  - Ensure the dependent package is approved by local site policy
  - Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop **vsftpd.service** and remove **vsftpd** package:

```
# systemctl stop vsftpd.service  
# dnf remove vsftpd
```

- OR -

- IF - the **vsftpd** package is required as a dependency:

Run the following commands to stop and mask the **vsftpd.service**:

```
# systemctl stop vsftpd.service  
# systemctl mask vsftpd.service
```

**Note:** Other ftp server packages may exist. If not required and authorized by local site policy, they should also be removed. If the package is required for a dependency, the service should be stopped and masked.

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230558  
Rule ID: SV-230558r627750  
STIG ID: RHEL-08-040360  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques                   | Tactics | Mitigations |
|-----------------------------------------------|---------|-------------|
| T1203.000, T1210, T1210.000, T1543, T1543.002 | TA0008  | M1042       |

## 2.1.7 Ensure message access server services are not in use (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

`dovecot` and `cyrus-imapd` are open source IMAP and POP3 server packages for Linux based systems.

### Rationale:

Unless POP3 and/or IMAP servers are to be provided by this system, it is recommended that the package be removed to reduce the potential attack surface.

**Note:** Several IMAP/POP3 servers exist and can use other service names. These should also be audited and the packages removed if not required.

### Impact:

There may be packages that are dependent on `dovecot` and `cyrus-imapd` packages. If `dovecot` and `cyrus-imapd` packages are removed, these dependent packages will be removed as well. Before removing `dovecot` and `cyrus-imapd` packages, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask `dovecot.socket`, `dovecot.service` and `cyrus-imapd.service` leaving `dovecot` and `cyrus-imapd` packages installed.

## Audit:

Run the following command to verify **dovecot** and **cyrus-imapd** are not installed:

```
# rpm -q dovecot cyrus-imapd

package dovecot is not installed
package cyrus-imapd is not installed
```

**- OR -**

**- IF -** a package is installed **and** is required for dependencies:

Run the following commands to verify **dovecot.socket**, **dovecot.service**, and **cyrus-imapd.service** are not enabled:

```
# systemctl is-enabled dovecot.socket dovecot.service cyrus-imapd.service
2>/dev/null | grep 'enabled'

Nothing should be returned
```

Run the following command to verify **dovecot.socket**, **dovecot.service**, and **cyrus-imapd.service** are not active:

```
# systemctl is-active dovecot.socket dovecot.service cyrus-imapd.service
2>/dev/null | grep '^active'

Nothing should be returned
```

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop **dovecot.socket**, **dovecot.service**, and **cyrus-imapd.service**, and remove **dovecot** and **cyrus-imapd** packages:

```
# systemctl stop dovecot.socket dovecot.service cyrus-imapd.service
# dnf remove dovecot cyrus-imapd
```

**- OR -**

**- IF -** a package is installed **and** is required for dependencies:

Run the following commands to stop and mask **dovecot.socket**, **dovecot.service**, and **cyrus-imapd.service**:

```
# systemctl stop dovecot.socket dovecot.service cyrus-imapd.service
# systemctl mask dovecot.socket dovecot.service cyrus-imapd.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                          | Tactics | Mitigations |
|------------------------------------------------------|---------|-------------|
| T1203, T1203.000, T1210, T1210.000, T1543, T1543.002 | TA0008  | M1042       |

## 2.1.8 Ensure network file system services are not in use (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The Network File System (NFS) is one of the first and most widely distributed file systems in the UNIX environment. It provides the ability for systems to mount file systems of other servers through the network.

### Rationale:

If the system does not require access to network shares or the ability to provide network file system services for other host's network shares, it is recommended that the `nfs-utils` package be removed to reduce the attack surface of the system.

### Impact:

Many of the `libvirt` packages used by Enterprise Linux virtualization are dependent on the `nfs-utils` package. If the `nfs-utils` package is removed, these dependent packages will be removed as well. Before removing the `nfs-utils` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the `nfs-server.service` leaving the `nfs-utils` package installed.



## Audit:

Run the following command to verify **nfs-utils** is not installed:

```
# rpm -q nfs-utils  
  
package nfs-utils is not installed
```

- **OR** - If package is required for dependencies:

Run the following command to verify that the **nfs-server.service** is not enabled:

```
# systemctl is-enabled nfs-server.service 2>/dev/null | grep 'enabled'  
  
Nothing should be returned
```

Run the following command to verify the **nfs-server.service** is not active:

```
# systemctl is-active nfs-server.service 2>/dev/null | grep '^active'  
  
Nothing should be returned
```

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following command to stop **nfs-server.service** and remove **nfs-utils** package:

```
# systemctl stop nfs-server.service  
# dnf remove nfs-utils
```

- **OR** -

- **IF** - the **nfs-utils** package is required as a dependency:

Run the following commands to stop and mask the **nfs-server.service**:

```
# systemctl stop nfs-server.service  
# systemctl mask nfs-server.service
```

## References:

1. NIST SP 800-53 :: CM-7
2. NIST SP 800-53A :: CM-7.1 (ii)

## Additional Information:

Many of the libvirt packages used by Enterprise Linux virtualization are dependent on the nfs-utils package. If the nfs-utils package is required as a dependency, the nfs-server service should be disabled and masked to reduce the attack surface of the system.

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                                                              | Tactics | Mitigations |
|------------------------------------------------------------------------------------------|---------|-------------|
| T1005, T1005.000, T1039, T1039.000, T1083, T1083.000, T1135, T1135.000, T1210, T1210.000 | TA0008  | M1042       |

## 2.1.9 Ensure nis server services are not in use (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client ( `ybind` ) was used to bind a machine to an NIS server and receive the distributed configuration files.

### Rationale:

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed.

### Impact:

There may be packages that are dependent on the `ypserv` package. If the `ypserv` package is removed, these dependent packages will be removed as well. Before removing the `ypserv` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the `ypserv.service` leaving the `ypserv` package installed.

## Audit:

Run the following command to verify **ypserv** is not installed:

```
# rpm -q ypserv  
  
package ypserv is not installed
```

**- OR -**

**- IF -** the package is required for dependencies:

Run the following command to verify **ypserv.service** is not enabled:

```
# systemctl is-enabled ypserv.service 2>/dev/null | grep 'enabled'  
  
Nothing should be returned
```

Run the following command to verify **ypserv.service** is not active:

```
# systemctl is-active ypserv.service 2>/dev/null | grep '^active'  
  
Nothing should be returned
```

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop **ypserv.service** and remove **ypserv** package:

```
# systemctl stop ypserv.service  
# dnf remove ypserv
```

**- OR -**

**- IF -** the **ypserv** package is required as a dependency:

Run the following commands to stop and mask **ypserv.service**:

```
# systemctl stop ypserv.service  
# systemctl mask ypserv.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                          | Tactics | Mitigations |
|------------------------------------------------------|---------|-------------|
| T1203, T1203.000, T1210, T1210.000, T1543, T1543.002 | TA0008  | M1042       |

## *2.1.10 Ensure print server services are not in use (Automated)*

### **Profile Applicability:**

- Level 1 - Server

### **Description:**

The Common Unix Print System (CUPS) provides the ability to print to both local and network printers. A system running CUPS can also accept print jobs from remote systems and print them to local printers. It also provides a web based remote administration capability.

### **Rationale:**

If the system does not need to print jobs or accept print jobs from other systems, it is recommended that CUPS be removed to reduce the potential attack surface.

### **Impact:**

Removing the cups package, or disabling `cups.socket` and/or `cups.service` will prevent printing from the system, a common task for workstation systems.

There may be packages that are dependent on the `cups` package. If the `cups` package is removed, these dependent packages will be removed as well. Before removing the `cups` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask `cups.socket` and `cups.service` leaving the `cups` package installed.

## Audit:

Run the following command to verify **cups** is not installed:

```
# rpm -q cups  
  
package cups is not installed
```

**- OR -**

**- IF -** the **cups** package is required as a dependency:

Run the following command to verify the **cups.socket** and **cups.service** are not enabled:

```
# systemctl is-enabled cups.socket cups.service 2>/dev/null | grep 'enabled'  
  
Nothing should be returned
```

Run the following command to verify the **cups.socket** and **cups.service** are not active:

```
# systemctl is-active cups.socket cups.service 2>/dev/null | grep '^active'  
  
Nothing should be returned
```

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop **cups.socket** and **cups.service**, and remove the **cups** package:

```
# systemctl stop cups.socket cups.service  
# dnf remove cups
```

**- OR -**

**- IF -** the **cups** package is required as a dependency:

Run the following commands to stop and mask the **cups.socket** and **cups.service**:

```
# systemctl stop cups.socket cups.service  
# systemctl mask cups.socket cups.service
```

## References:

1. <http://www.cups.org>
2. NIST SP 800-53 Rev. 5: CM-7

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                          | Tactics | Mitigations |
|------------------------------------------------------|---------|-------------|
| T1203, T1203.000, T1210, T1210.000, T1543, T1543.002 | TA0008  | M1042       |



## 2.1.11 Ensure rpcbind services are not in use (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The `rpcbind` utility maps RPC services to the ports on which they listen. RPC processes notify `rpcbind` when they start, registering the ports they are listening on and the RPC program numbers they expect to serve. The client system then contacts `rpcbind` on the server with a particular RPC program number. The `rpcbind.service` redirects the client to the proper port number so it can communicate with the requested service.

Portmapper is an RPC service, which always listens on tcp and udp 111, and is used to map other RPC services (such as nfs, nlockmgr, quotad, mountd, etc.) to their corresponding port number on the server. When a remote host makes an RPC call to that server, it first consults with portmap to determine where the RPC server is listening.

### Rationale:

A small request (~82 bytes via UDP) sent to the Portmapper generates a large response (7x to 28x amplification), which makes it a suitable tool for DDoS attacks. If `rpcbind` is not required, it is recommended to remove `rpcbind` package to reduce the potential attack surface.

### Impact:

Many of the libvirt packages used by Enterprise Linux virtualization, and the `nfs-utils` package used for The Network File System (NFS), are dependent on the `rpcbind` package. If the `rpcbind` package is removed, these dependent packages will be removed as well. Before removing the `rpcbind` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the `rpcbind.socket` and `rpcbind.service` leaving the `rpcbind` package installed.

## Audit:

Run the following command to verify **rpcbind** package is not installed:

```
# rpm -q rpcbind  
  
package rpcbind is not installed
```

- OR -

- IF - the **rpcbind** package is required as a dependency:

Run the following command to verify **rpcbind.socket** and **rpcbind.service** are not enabled:

```
# systemctl is-enabled rpcbind.socket rpcbind.service 2>/dev/null | grep  
'enabled'  
  
Nothing should be returned
```

Run the following command to verify **rpcbind.socket** and **rpcbind.service** are not active:

```
# systemctl is-active rpcbind.socket rpcbind.service 2>/dev/null | grep  
'^active'  
  
Nothing should be returned
```

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop **rpcbind.socket** and **rpcbind.service**, and remove the **rpcbind** package:

```
# systemctl stop rpcbind.socket rpcbind.service  
# dnf remove rpcbind
```

- OR -

- IF - the **rpcbind** package is required as a dependency:

Run the following commands to stop and mask the **rpcbind.socket** and **rpcbind.service**:

```
# systemctl stop rpcbind.socket rpcbind.service  
# systemctl mask rpcbind.socket rpcbind.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-7

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                                            | Tactics | Mitigations |
|------------------------------------------------------------------------|---------|-------------|
| T1203, T1203.000, T1210, T1210.000, T1498, T1498.002, T1543, T1543.002 | TA0008  | M1042       |

## 2.1.12 Ensure rsync services are not in use (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The **rsyncd.service** can be used to synchronize files between systems over network links.

### Rationale:

Unless required, the **rsync-daemon** package should be removed to reduce the potential attack surface.

The **rsyncd.service** presents a security risk as it uses unencrypted protocols for communication.

### Impact:

There may be packages that are dependent on the **rsync-daemon** package. If the **rsync-daemon** package is removed, these dependent packages will be removed as well. Before removing the **rsync-daemon** package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the **rsyncd.socket** and **rsyncd.service** leaving the **rsync-daemon** package installed.

## Audit:

Run the following command to verify the **rsync-daemon** package is not installed:

```
# rpm -q rsync-daemon  
  
package rsync-daemon is not installed
```

- OR -

- IF - the **rsync-daemon** package is required as a dependency:

Run the following command to verify **rsyncd.socket** and **rsyncd.service** are not enabled:

```
# systemctl is-enabled rsyncd.socket rsyncd.service 2>/dev/null | grep  
'enabled'  
  
Nothing should be returned
```

Run the following command to verify **rsyncd.socket** and **rsyncd.service** are not active:

```
# systemctl is-active rsyncd.socket rsyncd.service 2>/dev/null | grep  
'^active'  
  
Nothing should be returned
```

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop **rsyncd.socket** and **rsyncd.service**, and remove the **rsync-daemon** package:

```
# systemctl stop rsyncd.socket rsyncd.service  
# dnf remove rsync-daemon
```

- OR -

- IF - the **rsync-daemon** package is required as a dependency:

Run the following commands to stop and mask the **rsyncd.socket** and **rsyncd.service**:

```
# systemctl stop rsyncd.socket rsyncd.service  
# systemctl mask rsyncd.socket rsyncd.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-7

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                                                              | Tactics | Mitigations |
|------------------------------------------------------------------------------------------|---------|-------------|
| T1105, T1105.000, T1203, T1203.000, T1210, T1210.000, T1543, T1543.002, T1570, T1570.000 | TA0008  | M1042       |

## 2.1.13 Ensure samba file server services are not in use (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The Samba daemon allows system administrators to configure their Linux systems to share file systems and directories with Windows desktops. Samba will advertise the file systems and directories via the Server Message Block (SMB) protocol. Windows desktop users will be able to mount these directories and file systems as letter drives on their systems.

### Rationale:

If there is no need to mount directories and file systems to Windows systems, then this package can be removed to reduce the potential attack surface.

### Impact:

There may be packages that are dependent on the **samba** package. If the **samba** package is removed, these dependent packages will be removed as well. Before removing the **samba** package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the **smb.service** leaving the **samba** package installed.

## Audit:

Run the following command to verify **samba** package is not installed:

```
# rpm -q samba  
  
package samba is not installed
```

**- OR -**

**- IF -** the package is required for dependencies:

Run the following command to verify **smb.service** is not enabled:

```
# systemctl is-enabled smb.service 2>/dev/null | grep 'enabled'  
  
Nothing should be returned
```

Run the following command to verify the **smb.service** is not active:

```
# systemctl is-active smb.service 2>/dev/null | grep '^active'  
  
Nothing should be returned
```

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following command to stop **smb.service** and remove **samba** package:

```
# systemctl stop smb.service  
# dnf remove samba
```

**- OR -**

**- IF -** the **samba** package is required as a dependency:

Run the following commands to stop and mask the **smb.service**:

```
# systemctl stop smb.service  
# systemctl mask smb.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-7



**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                                                                                                  | Tactics | Mitigations |
|------------------------------------------------------------------------------------------------------------------------------|---------|-------------|
| T1005, T1005.000, T1039, T1039.000, T1083, T1083.000, T1135, T1135.000, T1203, T1203.000, T1210, T1210.000, T1543, T1543.002 | TA0008  | M1042       |

## 2.1.14 Ensure snmp services are not in use (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Simple Network Management Protocol (SNMP) is a widely used protocol for monitoring the health and welfare of network equipment, computer equipment and devices like UPSs.

Net-SNMP is a suite of applications used to implement SNMPv1 (RFC 1157), SNMPv2 (RFCs 1901-1908), and SNMPv3 (RFCs 3411-3418) using both IPv4 and IPv6.

Support for SNMPv2 classic (a.k.a. "SNMPv2 historic" - RFCs 1441-1452) was dropped with the 4.0 release of the UCD-snmp package.

The Simple Network Management Protocol (SNMP) server is used to listen for SNMP commands from an SNMP management system, execute the commands or collect the information and then send results back to the requesting system.

### Rationale:

The SNMP server can communicate using **SNMPv1**, which transmits data in the clear and does not require authentication to execute commands. **SNMPv3** replaces the simple/clear text password sharing used in **SNMPv2** with more securely encoded parameters. If the the SNMP service is not required, the **net-snmp** package should be removed to reduce the attack surface of the system.

**Note:** If SNMP is required:

- The server should be configured for **SNMP v3** only. **User Authentication** and **Message Encryption** should be configured.
- If **SNMP v2** is **absolutely** necessary, modify the community strings' values.

### Impact:

There may be packages that are dependent on the **net-snmp** package. If the **net-snmp** package is removed, these packages will be removed as well.

Before removing the **net-snmp** package, review any dependent packages to determine if they are required on the system. If a dependent package is required, stop and mask the **snmpd.service** leaving the **net-snmp** package installed.

## Audit:

Run the following command to verify **net-snmp** package is not installed:

```
# rpm -q net-snmp  
  
package net-snmp is not installed
```

- **OR** - If the package is required for dependencies:

Run the following command to verify the **snmpd.service** is not enabled:

```
# systemctl is-enabled snmpd.service 2>/dev/null | grep 'enabled'  
  
Nothing should be returned
```

Run the following command to verify the **snmpd.service** is not active:

```
# systemctl is-active snmpd.service 2>/dev/null | grep '^active'  
  
Nothing should be returned
```

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop **snmpd.service** and remove **net-snmp** package:

```
# systemctl stop snmpd.service  
# dnf remove net-snmp
```

- **OR** - If the package is required for dependencies:

Run the following commands to stop and mask the **snmpd.service**:

```
# systemctl stop snmpd.service  
# systemctl mask snmpd.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                          | Tactics | Mitigations |
|------------------------------------------------------|---------|-------------|
| T1203, T1203.000, T1210, T1210.000, T1543, T1543.002 | TA0008  | M1042       |

## 2.1.15 Ensure telnet server services are not in use (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

### Description:

The `telnet-server` package contains the `telnet` daemon, which accepts connections from users from other systems via the `telnet` protocol.

### Rationale:

The `telnet` protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow a user with access to sniff network traffic the ability to steal credentials. The `ssh` package provides an encrypted session and stronger security.

### Impact:

There may be packages that are dependent on the `telnet-server` package. If the `telnet-server` package is removed, these dependent packages will be removed as well. Before removing the `telnet-server` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the `telnet.socket` leaving the `telnet-server` package installed.

## Audit:

Run the following command to verify the **telnet-server** package is not installed:

```
rpm -q telnet-server  
  
package telnet-server is not installed
```

**- OR -**

**- IF -** a package is installed **and** is required for dependencies:

Run the following command to verify **telnet.socket** is not enabled:

```
# systemctl is-enabled telnet.socket 2>/dev/null | grep 'enabled'  
  
Nothing should be returned
```

Run the following command to verify **telnet.socket** is not active:

```
# systemctl is-active telnet.socket 2>/dev/null | grep '^active'  
  
Nothing should be returned
```

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop **telnet.socket** and remove the **telnet-server** package:

```
# systemctl stop telnet.socket  
# dnf remove telnet-server
```

**- OR -**

**- IF -** a package is installed **and** is required for dependencies:

Run the following commands to stop and mask **telnet.socket**:

```
# systemctl stop telnet.socket  
# systemctl mask telnet.socket
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7, CM-11
2. NIST SP 800-53A :: CM-7.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230487  
Rule ID: SV-230487r627750  
STIG ID: RHEL-08-040000  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      | ●    | ●    |
| v7               | <b>2.6 <u>Address unapproved software</u></b><br>Ensure that unauthorized software is either removed or the inventory is updated in a timely manner                                                                                                                | ●    | ●    | ●    |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques                          | Tactics | Mitigations |
|------------------------------------------------------|---------|-------------|
| T1203, T1203.000, T1210, T1210.000, T1543, T1543.002 | TA0008  | M1042       |

## 2.1.16 Ensure tftp server services are not in use (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Trivial File Transfer Protocol (TFTP) is a simple protocol for exchanging files between two TCP/IP machines. TFTP servers allow connections from a TFTP Client for sending and receiving files.

### Rationale:

Unless there is a need to run the system as a TFTP server, it is recommended that the package be removed to reduce the potential attack surface.

TFTP does not have built-in encryption, access control or authentication. This makes it very easy for an attacker to exploit TFTP to gain access to files

### Impact:

TFTP is often used to provide files for network booting such as for PXE based installation of servers.

There may be packages that are dependent on the `tftp-server` package. If the `tftp-server` package is removed, these dependent packages will be removed as well. Before removing the `tftp-server` package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the `tftp.socket` and `tftp.service` leaving the `tftp-server` package installed.



## Audit:

Run the following command to verify **tftp-server** is not installed:

```
# rpm -q tftp-server  
  
package tftp-server is not installed
```

**- OR -**

**- IF -** the package is required for dependencies:

Run the following command to verify **tftp.socket** and **tftp.service** are not enabled:

```
# systemctl is-enabled tftp.socket tftp.service 2>/dev/null | grep 'enabled'  
  
Nothing should be returned
```

Run the following command to verify the **tftp.socket** and **tftp.service** are not active:

```
# systemctl is-active tftp.socket tftp.service 2>/dev/null | grep '^active'  
  
Nothing should be returned
```

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop **tftp.socket** and **tftp.service**, and remove the **tftp-server** package:

```
# systemctl stop tftp.socket tftp.service  
# dnf remove tftp-server
```

**- OR -**

**- IF -** the **tftp-server** package is required as a dependency:

Run the following commands to stop and mask **tftp.socket** and **tftp.service**:

```
# systemctl stop tftp.socket tftp.service  
# systemctl mask tftp.socket tftp.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                          | Tactics | Mitigations |
|------------------------------------------------------|---------|-------------|
| T1203, T1203.000, T1210, T1210.000, T1543, T1543.002 | TA0008  | M1042       |

## *2.1.17 Ensure web proxy server services are not in use (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Squid is a standard proxy server used in many distributions and environments.

### **Rationale:**

Unless a system is specifically set up to act as a proxy server, it is recommended that the squid package be removed to reduce the potential attack surface.

**Note:** Several HTTP proxy servers exist. These should be checked and removed unless required.

### **Impact:**

There may be packages that are dependent on the **squid** package. If the **squid** package is removed, these dependent packages will be removed as well. Before removing the **squid** package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the **squid.service** leaving the **squid** package installed.

## Audit:

Run the following command to verify **squid** package is not installed:

```
# rpm -q squid  
  
package squid is not installed
```

- OR -

- IF - the package is required for dependencies:

Run the following command to verify **squid.service** is not enabled:

```
# systemctl is-enabled squid.service 2>/dev/null | grep 'enabled'  
  
Nothing should be returned
```

Run the following command to verify the **squid.service** is not active:

```
# systemctl is-active squid.service 2>/dev/null | grep '^active'  
  
Nothing should be returned
```

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop **squid.service** and remove the **squid** package:

```
# systemctl stop squid.service  
# dnf remove squid
```

- OR - If the **squid** package is required as a dependency:

Run the following commands to stop and mask the **squid.service**:

```
# systemctl stop squid.service  
# systemctl mask squid.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-6, CM-7

## Additional Information:

Several HTTP proxy servers exist. These and other services should be checked.

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                          | Tactics | Mitigations |
|------------------------------------------------------|---------|-------------|
| T1203, T1203.000, T1210, T1210.000, T1543, T1543.002 | TA0008  | M1042       |

## *2.1.18 Ensure web server services are not in use (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Web servers provide the ability to host web site content.

### **Rationale:**

Unless there is a local site approved requirement to run a web server service on the system, web server packages should be removed to reduce the potential attack surface.

### **Impact:**

Removal of web server packages will remove that ability for the server to host web services.

- **IF** - the web server package is required for a dependency, any related service or socket should be stopped and masked.

**Note:** If the remediation steps to mask a service are followed and that package is not installed on the system, the service and/or socket will still be masked. If the package is installed due to an approved requirement to host a web server, the associated service and/or socket would need to be unmasked before it could be enabled and/or started.

## Audit:

Run the following command to verify **httpd** and **nginx** are not installed:

```
# rpm -q httpd nginx  
  
package httpd is not installed  
package nginx is not installed
```

**- OR -**

**- IF -** a package is installed **and** is required for dependencies:

Run the following command to verify **httpd.socket**, **httpd.service**, and **nginx.service** are not enabled:

```
# systemctl is-enabled httpd.socket httpd.service nginx.service 2>/dev/null |  
grep 'enabled'  
  
Nothing should be returned
```

Run the following command to verify **httpd.socket**, **httpd.service**, and **nginx.service** are not active:

```
# systemctl is-active httpd.socket httpd.service nginx.service 2>/dev/null |  
grep '^active'  
  
Nothing should be returned
```

## Note:

- Other web server packages may exist. They should also be audited, if not required and authorized by local site policy
- If the package is required for a dependency:
  - Ensure the dependent package is approved by local site policy
  - Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop **httpd.socket**, **httpd.service**, and **nginx.service**, and remove **httpd** and **nginx** packages:

```
# systemctl stop httpd.socket httpd.service nginx.service
# dnf remove httpd nginx
```

- OR -

- IF - a package is installed **and** is required for dependencies:

Run the following commands to stop and mask **httpd.socket**, **httpd.service**, and **nginx.service**:

```
# systemctl stop httpd.socket httpd.service nginx.service
# systemctl mask httpd.socket httpd.service nginx.service
```

**Note:** Other web server packages may exist. If not required and authorized by local site policy, they should also be removed. If the package is required for a dependency, the service and socket should be stopped and masked.

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      | ●    | ●    |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques                          | Tactics | Mitigations |
|------------------------------------------------------|---------|-------------|
| T1203, T1203.000, T1210, T1210.000, T1543, T1543.002 | TA0008  | M1042       |



## 2.1.19 Ensure xinetd services are not in use (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The eXtended InterNET Daemon (**xinetd**) is an open source super daemon that replaced the original **inetd** daemon. The **xinetd** daemon listens for well known services and dispatches the appropriate daemon to properly respond to service requests.

### Rationale:

If there are no **xinetd** services required, it is recommended that the package be removed to reduce the attack surface area of the system.

**Note:** If an **xinetd** service or services are required, ensure that any **xinetd** service not required is stopped and masked

### Impact:

There may be packages that are dependent on the **xinetd** package. If the **xinetd** package is removed, these dependent packages will be removed as well. Before removing the **xinetd** package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the avahi-daemon.socket and avahi-daemon.service leaving the avahi package installed.

## Audit:

Run the following command to verify the **xinetd** package is not installed:

```
# rpm -q xinetd  
  
package xinetd is not installed
```

- OR -

- IF - the **xinetd** package is required as a dependency:

Run the following command to verify **xinetd.service** is not enabled:

```
# systemctl is-enabled xinetd.service 2>/dev/null | grep 'enabled'  
  
Nothing should be returned
```

Run the following command to verify **xinetd.service** is not active:

```
# systemctl is-active xinetd.service 2>/dev/null | grep '^active'  
  
Nothing should be returned
```

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop **xinetd.service**, and remove the **xinetd** package:

```
# systemctl stop xinetd.service  
# dnf remove xinetd
```

- OR -

- IF - the **xinetd** package is required as a dependency:

Run the following commands to stop and mask the **xinetd.service**:

```
# systemctl stop xinetd.service  
# systemctl mask xinetd.service
```

## References:

1. NIST SP 800-53 Rev. 5: CM-7

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                          | Tactics | Mitigations |
|------------------------------------------------------|---------|-------------|
| T1203, T1203.000, T1210, T1210.000, T1543, T1543.002 | TA0008  | M1042       |

## 2.1.20 Ensure X window server services are not in use (Automated)

### Profile Applicability:

- Level 2 - Server
- STIG

### Description:

The X Window System provides a Graphical User Interface (GUI) where users can have multiple windows in which to run programs and various add on. The X Windows system is typically used on workstations where users login, but not on servers where users typically do not login.

### Rationale:

Unless your organization specifically requires graphical login access via X Windows, remove it to reduce the potential attack surface.

### Impact:

If a Graphical Desktop Manager (GDM) is in use on the system, there may be a dependency on the **xorg-x11-server-common** package. If the GDM is required and approved by local site policy, the package should **not** be removed.

Many Linux systems run applications which require a Java runtime. Some Linux Java packages have a dependency on specific X Windows xorg-x11-fonts. One workaround to avoid this dependency is to use the "headless" Java packages for your specific Java runtime.

### Audit:

- **IF** - a Graphical Desktop Manager or X-Windows server is not required and approved by local site policy:

Run the following command to Verify X Windows Server is not installed.

```
# rpm -q xorg-x11-server-common  
package xorg-x11-server-common is not installed
```

**Remediation:**

- **IF** - a Graphical Desktop Manager or X-Windows server is not required and approved by local site policy:

Run the following command to remove the X Windows Server packages:

```
# dnf remove xorg-x11-server-common
```

**References:**

- 1. NIST SP 800-53 :: CM-6 b
- 2. NIST SP 800-53A :: CM-6.1 (iv)

**Additional Information:**

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230553  
Rule ID: SV-230553r809324  
STIG ID: RHEL-08-040320  
Severity: CAT II

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2        | IG 3        |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------|-------------|
| v8               | 4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      | <div></div> | <div></div> |
| v7               | 9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      | <div></div> | <div></div> |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                          | Tactics | Mitigations |
|------------------------------------------------------|---------|-------------|
| T1203, T1203.000, T1210, T1210.000, T1543, T1543.002 | TA0008  | M1042       |

## *2.1.21 Ensure only approved services are listening on a network interface (Manual)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

A network port is identified by its number, the associated IP address, and the type of the communication protocol such as TCP or UDP.

A listening port is a network port on which an application or process listens on, acting as a communication endpoint.

Each listening port can be open or closed (filtered) using a firewall. In general terms, an open port is a network port that accepts incoming packets from remote locations.

### **Rationale:**

Services listening on the system pose a potential risk as an attack vector. These services should be reviewed, and if not required, the service should be stopped, and the package containing the service should be removed. If required packages have a dependency, the service should be stopped and masked to reduce the attack surface of the system.

### **Impact:**

There may be packages that are dependent on the service's package. If the service's package is removed, these dependent packages will be removed as well. Before removing the service's package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask the `<service_name>.socket` and `<service_name>.service` leaving the service's package installed.

## Audit:

Run the following command:

```
# ss -plntu
```

Review the output to ensure:

- All services listed are required on the system and approved by local site policy.
- Both the port and interface the service is listening on are approved by local site policy.
- If a listed service is not required:
  - Remove the package containing the service
  - **- IF -** the service's package is required for a dependency, stop and mask the service and/or socket

## Remediation:

Run the following commands to stop the service and remove the package containing the service:

```
# systemctl stop <service_name>.socket <service_name>.service
# dnf remove <package_name>
```

**- OR -** If required packages have a dependency:

Run the following commands to stop and mask the service and socket:

```
# systemctl stop <service_name>.socket <service_name>.service
# systemctl mask <service_name>.socket <service_name>.service
```

**Note:** replace **<service\_name>** with the appropriate service name.

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                          | Tactics | Mitigations |
|------------------------------------------------------|---------|-------------|
| T1203, T1203.000, T1210, T1210.000, T1543, T1543.002 | TA0008  | M1042       |



## 2.1.22 *Ensure automated bug reporting tools are not installed (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The operating system must not have any automated bug reporting tools installed.

### **Rationale:**

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, games, software packages, tools, and demonstration software not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

Verify the operating system is configured to disable non-essential capabilities. The most secure way of ensuring a non-essential capability is disabled is to not have the capability installed.

### **Audit:**

Check to see if any automated bug reporting packages are installed with the following command:

```
# dnf list installed abrt*
```

If any automated bug reporting package is installed, this is a finding.

### **Remediation:**

Configure the operating system to disable non-essential capabilities by removing automated bug reporting packages from the system with the following command:

```
# dnf remove abrt*
```

### **References:**

1. NIST SP 800-53 Revision 4 :: CM-7 a NIST SP 800-53 Revision 5 :: CM-7 a
2. NIST SP 800-53A :: CM-7.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230488  
Rule ID: SV-230488r627750  
STIG ID: RHEL-08-040001  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

### *2.1.23 Ensure mail transfer agents are configured for local-only mode (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Mail Transfer Agents (MTA), such as sendmail and Postfix, are used to listen for incoming mail and transfer the messages to the appropriate user or mail server. If the system is not intended to be a mail server, it is recommended that the MTA be configured to only process local mail.

#### **Rationale:**

The software for all Mail Transfer Agents is complex and most have a long history of security issues. While it is important to ensure that the system can process local mail messages, it is not necessary to have the MTA's daemon listening on a port unless the server is intended to be a mail server that receives and processes mail from other systems.

## Audit:

Run the following script to verify that the MTA is not listening on any non-loopback address ( 127.0.0.1 or ::1):

```
#!/usr/bin/env bash

{
    a_output=(); a_output2=(); a_port_list=("25" "465" "587")
    for l_port_number in "${a_port_list[@]}"; do
        if ss -plntu | grep -P -- ':"$l_port_number"\b' | grep -Pvq --
        '\h+(127\.0\.0\.1|1\.[?::1\])?:"$l_port_number"\b'; then
            a_output2+=(" - Port \"$l_port_number\" is listening on a non-
loopback network interface")
        else
            a_output+=(" - Port \"$l_port_number\" is not listening on a non-
loopback network interface")
        fi
    done
    if command -v postconf &> /dev/null; then
        l_interfaces="$(postconf -n inet_interfaces)"
    elif command -v exim &> /dev/null; then
        l_interfaces="$(exim -bP local_interfaces)"
    elif command -v sendmail &> /dev/null; then
        l_interfaces="$(grep -i "0 DaemonPortOptions=" /etc/mail/sendmail.cr |
grep -oP '?<=Addr=) [^,++]' )"
    fi
    if [ -n "$l_interfaces" ]; then
        if grep -Pqi '\ball\b' <<< "$l_interfaces"; then
            a_output2+=(" - MTA is bound to all network interfaces")
        elif ! grep -Pqi '(inet_interfaces\h*=\h*)?(0\0\0\0|::1|loopback-
only)' <<< "$l_interfaces"; then
            a_output2+=(" - MTA is bound to a network interface" "
\"$l_interfaces\"")
        else
            a_output+=(" - MTA is not bound to a non loopback network interface"
" \" $l_interfaces\"")
        fi
    else
        a_output+=(" - MTA not detected or in use")
    fi
    if [ "${#a_output2[@]}" -le 0 ]; then
        printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}"
    else
        printf '%s\n' "" "- Audit Result:" " ** FAIL **" " * Reasons for
audit failure *" "${a_output2[@]}" ""
        [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "- Correctly set:"
"${a_output[@]}"
    fi
}
```

## Remediation:

Edit `/etc/postfix/main.cf` and add the following line to the RECEIVING MAIL section. If the line already exists, change it to look like the line below:

```
inet_interfaces = loopback-only
```

Run the following command to restart `postfix`:

```
# systemctl restart postfix
```

## Note:

- This remediation is designed around the postfix mail server.
- Depending on your environment you may have an alternative MTA installed such as sendmail. If this is the case consult the documentation for your installed MTA to configure the recommended state.

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      | ●    | ●    |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1018, T1018.000, T1210, T1210.000 | TA0008  | M1042       |

## 2.1.24 Ensure the sendmail package is not installed (Automated)

### Profile Applicability:

- STIG

### Description:

The operating system must not have the sendmail package installed.

### Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Examples of non-essential capabilities include, but are not limited to, games, software packages, tools, and demonstration software not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

Verify the operating system is configured to disable non-essential capabilities. The most secure way of ensuring a non-essential capability is disabled is to not have the capability installed.

### Audit:

Check to see if the sendmail package is installed with the following command:

```
# dnf list installed sendmail
```

If the sendmail package is installed, this is a finding.

### Remediation:

Configure the operating system to disable non-essential capabilities by removing the sendmail package from the system with the following command:

```
# dnf remove sendmail
```

### References:

1. NIST SP 800-53 Revision 5 :: CM-7 a
2. NIST SP 800-53A :: CM-7.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230489  
Rule ID: SV-230489r627750  
STIG ID: RHEL-08-040002  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## 2.1.25 Ensure the rsh-server package is not installed (Automated)

### Profile Applicability:

- STIG

### Description:

The operating system must not have the rsh-server package installed.

### Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

The rsh-server service provides an unencrypted remote access service that does not provide for the confidentiality and integrity of user passwords or the remote session and has very weak authentication.

If a privileged user were to log on using this service, the privileged user password could be compromised.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000074-GPOS-00042

### Audit:

Check to see if the rsh-server package is installed with the following command:

```
# dnf list installed rsh-server
```

If the rsh-server package is installed, this is a finding.

### Remediation:

Configure the operating system to disable non-essential capabilities by removing the rsh-server package from the system with the following command:

```
# dnf remove rsh-server
```

### References:

1. NIST SP 800-53 Revision 5 :: CM-7 a
2. NIST SP 800-53A :: CM-7.1 (ii)



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230492  
Rule ID: SV-230492r627750  
STIG ID: RHEL-08-040010  
Severity: CAT I

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## 2.1.26 Ensure system daemons are prevented from using Kerberos for authentication (Automated)

### Profile Applicability:

- STIG

### Description:

Kerberos is a passwordless computer network security authentication protocol that was created by MIT to help solve network security problems

### Rationale:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised.

Operating systems utilizing encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

The key derivation function (KDF) in Kerberos is not FIPS compatible. Ensuring the system does not have any keytab files present prevents system daemons from using Kerberos for authentication. A keytab is a file containing pairs of Kerberos principals and encrypted keys.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general-purpose computing system.

### Audit:

- **IF** - the system is a server utilizing krb5-server-1.17-18.el8.x86\_64 - **OR** - the system is a workstation utilizing krb5-workstation-1.17-18.el8.x86\_64 or newer, this requirement is not applicable.

Run the following command to verify there are no available keytab files:

```
# find /etc -mount -maxdepth 1 -type f -name '*.keytab'
```

Nothing should be returned

**Remediation:**

Configure the operating system to prevent system daemons from using Kerberos for authentication.

Run the following command to remove any files with the .keytab extension from the operating system:

```
# find /etc -mount -maxdepth 1 -type f -name '*.keytab' -exec rm -f {} +
```

**References:**

- 1. NIST SP 800-53 :: IA-7
- 2. NIST SP 800-53A :: IA-7.1

**Additional Information:**

Red Hat Enterprise Linux 8

Red Hat Enterprise Linux 8 STIG  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024  
  
GROUP ID: V-230238  
RULE ID: SV-230238r646862  
STIG ID: RHEL-08-010161  
SEVERITY: CAT II

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## 2.1.27 Ensure the operating system is configured to mask the debug-shell systemd service (Automated)

### Profile Applicability:

- STIG

### Description:

The debug-shell systemd service must be disabled.

### Rationale:

The debug-shell requires no authentication and provides root privileges to anyone who has physical access to the machine. While this feature is disabled by default, masking it adds an additional layer of assurance that it will not be enabled via a dependency in systemd. This also prevents attackers with physical access from trivially bypassing security on the machine through valid troubleshooting configurations and gaining root access when the system is rebooted.

### Audit:

Verify the operating system is configured to mask the debug-shell systemd service with the following command:

```
# systemctl status debug-shell.service

debug-shell.service
Loaded: masked (Reason: Unit debug-shell.service is masked.)
Active: inactive (dead)
```

If the "debug-shell.service" is loaded and not masked, this is a finding.

### Remediation:

Configure the system to mask the debug-shell systemd service with the following command:

```
# systemctl mask debug-shell.service

Created symlink /etc/systemd/system/debug-shell.service -> /dev/null
```

Reload the daemon to take effect.

```
# systemctl daemon-reload
```

### References:

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230532  
Rule ID: SV-230532r627750  
STIG ID: RHEL-08-040180  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## *2.1.28 Ensure the gssproxy package has not been installed on the system (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The gssproxy package must not be installed unless it is mission essential.

### **Rationale:**

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

The gssproxy package is a proxy for GSS API credential handling and could expose secrets on some networks. It is not needed for normal function of the OS.

### **Audit:**

Verify the gssproxy package has not been installed on the system with the following commands:

```
# dnf list installed gssproxy  
  
gssproxy.x86_64 0.8.0-14.el8 @anaconda
```

If the gssproxy package is installed and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

### **Remediation:**

Document the gssproxy package with the ISSO as an operational requirement or remove it from the system with the following command:

```
# dnf remove gssproxy
```

### **References:**

1. NIST SP 800-53 :: CM-7
2. NIST SP 800-53A :: CM-7.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230559  
Rule ID: SV-230559r646887  
STIG ID: RHEL-08-040370  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## 2.1.29 Ensure the *iprutils* package has not been installed on the system (Automated)

### Profile Applicability:

- STIG

### Description:

The *iprutils* package must not be installed unless it is mission essential.

### Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

The *iprutils* package provides a suite of utilities to manage and configure SCSI devices supported by the *ipr* SCSI storage device driver.

### Audit:

Verify the *iprutils* package has not been installed on the system with the following commands:

```
# dnf list installed iprutils  
  
iprutils.x86_64 2.4.18.1-1.el8 @anaconda
```

If the *iprutils* package is installed and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

### Remediation:

Document the *iprutils* package with the ISSO as an operational requirement or remove it from the system with the following command:

```
# dnf remove iprutils
```

### References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230560  
Rule ID: SV-230560r627750  
STIG ID: RHEL-08-040380  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## *2.1.30 Ensure the krb5-server package has not been installed on the system (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The krb5-server package must not be installed.

### **Rationale:**

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised.

RHEL 8 operating systems utilizing encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

Currently, Kerberos does not utilize FIPS 140-2 cryptography.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general-purpose computing system.

### **Audit:**

Verify the krb5-server package has not been installed on the system with the following commands:

If the system is a workstation or is utilizing krb5-server-1.17-18.el8.x86\_64 or newer, this is Not Applicable

```
# dnf list installed krb5-server  
  
krb5-server.x86_64 1.17-9.el8 repository
```

If the krb5-server package is installed and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

### **Remediation:**

Document the krb5-server package with the ISSO as an operational requirement or remove it from the system with the following command:

```
# dnf remove krb5-server
```

### **References:**

1. NIST SP 800-53 :: IA-7
2. NIST SP 800-53A :: IA-7.1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-237640  
Rule ID: SV-237640r646890  
STIG ID: RHEL-08-010163  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## *2.1.31 Ensure a TFTP server has not been installed on the system (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The Trivial File Transfer Protocol (TFTP) server package must not be installed if not required for operational support.

### **Rationale:**

If TFTP is required for operational support (such as the transmission of router configurations) its use must be documented with the Information System Security Officer (ISSO), restricted to only authorized personnel, and have access control rules established.

### **Audit:**

Verify a TFTP server has not been installed on the system with the following command:

```
# dnf list installed tftp-server  
  
tftp-server.x86_64 5.2-24.el8
```

If TFTP is installed and the requirement for TFTP is not documented with the ISSO, this is a finding.

### **Remediation:**

Remove the TFTP package from the system with the following command:

```
# dnf remove tftp-server
```

### **References:**

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230533  
Rule ID: SV-230533r627750  
STIG ID: RHEL-08-040190  
Severity: CAT I

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## 2.1.32 Ensure the tuned package has not been installed on the system (Automated)

### Profile Applicability:

- STIG

### Description:

The tuned package must not be installed unless it is mission essential.

### Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

The tuned package contains a daemon that tunes the system settings dynamically. It does so by monitoring the usage of several system components periodically. Based on that information, components will then be put into lower or higher power savings modes to adapt to the current usage. The tuned package is not needed for normal OS operations.

### Audit:

Verify the tuned package has not been installed on the system with the following commands:

```
# dnf list installed tuned
tuned.noarch 2.12.0-3.el8 @anaconda
```

If the tuned package is installed and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

### Remediation:

Document the tuned package with the ISSO as an operational requirement or remove it from the system with the following command:

```
# dnf remove tuned
```

### References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230561  
Rule ID: SV-230561r627750  
STIG ID: RHEL-08-040390  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

### *2.1.33 Ensure the operating system has enabled the hardware random number generator entropy gatherer service (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must enable the hardware random number generator entropy gatherer service.

#### **Rationale:**

The most important characteristic of a random number generator is its randomness, namely its ability to deliver random numbers that are impossible to predict. Entropy in computer security is associated with the unpredictability of a source of randomness. The random source with high entropy tends to achieve a uniform distribution of random values. Random number generators are one of the most important building blocks of cryptosystems.

The rngd service feeds random data from hardware device to kernel random device. Quality (non-predictable) random number generation is important for several security functions (i.e., ciphers).

#### **Audit:**

Check that the operating system has enabled the hardware random number generator entropy gatherer service.

Verify the rngd service is enabled and active with the following commands:

```
# systemctl is-enabled rngd
enabled

# systemctl is-active rngd
active
```

If the service is not "enable and "active", this is a finding.

#### **Remediation:**

Start the rngd service, and enable the rngd service with the following commands:

```
# systemctl start rngd.service
# systemctl enable rngd.service
```



## References:

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230285  
Rule ID: SV-230285r928587  
STIG ID: RHEL-08-010471  
Severity: CAT III

## CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

## 2.1.34 Ensure the operating system is configured to prevent unrestricted mail relaying (Automated)

### Profile Applicability:

- STIG

### Description:

The operating system must be configured to prevent unrestricted mail relaying.

### Rationale:

If unrestricted mail relaying is permitted, unauthorized senders could use this host as a mail relay for the purpose of sending spam or other unauthorized activity.

### Audit:

Verify the system is configured to prevent unrestricted mail relaying.  
Determine if "postfix" is installed with the following commands:

```
# dnf list installed postfix  
  
postfix.x86_64 2:3.3.1-9.el8
```

If postfix is not installed, this is Not Applicable.

If postfix is installed, determine if it is configured to reject connections from unknown or untrusted networks with the following command:

```
# postconf -n smtpd_client_restrictions  
  
smtpd_client_restrictions = permit_mynetworks, reject
```

If the "smtpd\_client\_restrictions" parameter contains any entries other than "permit\_mynetworks" and "reject", this is a finding.

### Remediation:

If "postfix" is installed, modify the "/etc/postfix/main.cf" file to restrict client connections to the local network with the following command:

```
# postconf -e 'smtpd_client_restrictions = permit_mynetworks,reject'
```

### References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230550  
Rule ID: SV-230550r627750  
STIG ID: RHEL-08-040290  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## 2.1.35 Ensure the TFTP daemon is configured to operate in secure mode (Automated)

### Profile Applicability:

- STIG

### Description:

If the Trivial File Transfer Protocol (TFTP) server is required, the TFTP daemon must be configured to operate in secure mode.

### Rationale:

Restricting TFTP to a specific directory prevents remote users from copying, transferring, or overwriting system files.

### Audit:

Verify the TFTP daemon is configured to operate in secure mode with the following commands:

```
# dnf list installed tftp-server  
tftp-server.x86_64 x.x-x.el8
```

If a TFTP server is not installed, this is Not Applicable.

If a TFTP server is installed, check for the server arguments with the following command:

```
# grep server_args /etc/xinetd.d/tftp  
server_args = -s /var/lib/tftpboot
```

If the "server\_args" line does not have a "-s" option, and a subdirectory is not assigned, this is a finding.

### Remediation:

Configure the TFTP daemon to operate in secure mode by adding the following line to "/etc/xinetd.d/tftp" (or modify the line to have the required value):

```
server_args = -s /var/lib/tftpboot
```

### References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230557  
Rule ID: SV-230557r627750  
STIG ID: RHEL-08-040350  
Severity: CAT II

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

## 2.2 Configure Client Services

A number of insecure services exist. While disabling the servers prevents a local attack against these services, it is advised to remove their clients unless they are required.

**Note:** This should not be considered a comprehensive list of insecure service clients. You may wish to consider additions to those listed here for your environment.

## 2.2.1 Ensure ftp client is not installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

FTP (File Transfer Protocol) is a traditional and widely used standard tool for transferring files between a server and clients over a network, especially where no authentication is necessary (permits anonymous users to connect to a server).

### Rationale:

FTP does not protect the confidentiality of data or authentication credentials. It is recommended SFTP be used if file transfer is required. Unless there is a need to run the system as a FTP server (for example, to allow anonymous downloads), it is recommended that the package be removed to reduce the potential attack surface.

### Audit:

Run the following command to verify **ftp** is not installed:

```
# rpm -q ftp  
package ftp is not installed
```

### Remediation:

Run the following command to remove **ftp**:

```
# dnf remove ftp
```

### References:

1. NIST SP 800-53 Rev. 5: CM-7

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1203, T1203.000, T1543, T1543.002 | TA0008  | M1042       |



## 2.2.2 Ensure ldap client is not installed (Automated)

### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

### Description:

The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service that provides a method for looking up information from a central database.

### Rationale:

If the system will not need to act as an LDAP client, it is recommended that the software be removed to reduce the potential attack surface.

### Impact:

Removing the LDAP client will prevent or inhibit using LDAP for authentication in your environment.

### Audit:

Run the following command to verify that the **openldap-clients** package is not installed:

```
# rpm -q openldap-clients  
package openldap-clients is not installed
```

### Remediation:

Run the following command to remove the **openldap-clients** package:

```
# dnf remove openldap-clients
```

### References:

1. NIST SP 800-53 Rev. 5: CM-7

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |                                                                                     |  |  |
| v7               | <b><u>2.6 Address unapproved software</u></b><br>Ensure that unauthorized software is either removed or the inventory is updated in a timely manner                                                                                                                |  |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1203, T1203.000, T1543, T1543.002 | TA0008  | M1042       |

### 2.2.3 Ensure nis client is not installed (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client ( **ypbind** ) was used to bind a machine to an NIS server and receive the distributed configuration files.

#### Rationale:

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed.

#### Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

#### Audit:

Run the following command to verify that the **ypbind** package is not installed:

```
# rpm -q ypbind  
package ypbind is not installed
```

#### Remediation:

Run the following command to remove the ypbind package:

```
# dnf remove ypbind
```

#### References:

1. NIST SP 800-53 Rev. 5: CM-7

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1203, T1203.000, T1543, T1543.002 | TA0008  | M1042       |

## 2.2.4 Ensure telnet client is not installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The **telnet** package contains the **telnet** client, which allows users to start connections to other systems via the telnet protocol.

### Rationale:

The **telnet** protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow an unauthorized user to steal credentials. The **ssh** package provides an encrypted session and stronger security and is included in most Linux distributions.

### Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

### Audit:

Run the following command to verify that the **telnet** package is not installed:

```
# rpm -q telnet  
  
package telnet is not installed
```

### Remediation:

Run the following command to remove the **telnet** package:

```
# dnf remove telnet
```

### References:

1. NIST SP 800-53 Rev. 5: CM-7

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |                                                                                     |  |  |
| v7               | <b><u>2.6 Address unapproved software</u></b><br>Ensure that unauthorized software is either removed or the inventory is updated in a timely manner                                                                                                                |  |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques                          | Tactics        | Mitigations  |
|------------------------------------------------------|----------------|--------------|
| T1040, T1040.000, T1203, T1203.000, T1543, T1543.002 | TA0006, TA0008 | M1041, M1042 |

## 2.2.5 Ensure *tftp* client is not installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Trivial File Transfer Protocol (TFTP) is a simple protocol for exchanging files between two TCP/IP machines. TFTP servers allow connections from a TFTP Client for sending and receiving files.

### Rationale:

TFTP does not have built-in encryption, access control or authentication. This makes it very easy for an attacker to exploit TFTP to gain access to files

### Audit:

Run the following command to verify **tftp** is not installed:

```
# rpm -q tftp  
package tftp is not installed
```

### Remediation:

Run the following command to remove **tftp**:

```
# dnf remove tftp
```

### References:

1. NIST SP 800-53 Rev. 5: CM-7

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1203, T1203.000, T1543, T1543.002 | TA0008  | M1042       |



## 2.2.6 Ensure krb5-workstation is not installed (Automated)

### Profile Applicability:

- STIG

### Description:

Kerberos is a network authentication system. The krb5-workstation package contains the basic Kerberos programs **kinit**, **klist**, **kdestroy**, **kpasswd**.

### Rationale:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity.

Operating systems utilizing encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

Currently, Kerberos does not utilize FIPS 140-2 cryptography.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general-purpose computing system.

### Impact:

This package may be required for Kerberos authentication

### Audit:

Verify the krb5-workstation package has not been installed on the system with the following commands:

If the system is a server or is utilizing krb5-workstation-1.17-18.el8.x86\_64 or newer, this is Not Applicable.

Run the following command to verify the **krb5-workstation** package is not installed -  
**OR** - version 1.17-18 or later

```
# rpm -q krb5-workstation
```

### Example output:

```
package krb5-workstation is not installed
- OR -
krb5-workstation-1.17-18.el8.x86_64
```

**Note:** If the krb5-workstation package is installed verify that it is documented and approved by local site policy

**Remediation:**

Document the krb5-workstation package with the ISSO as an operational requirement or remove it from the system with the following command:  
Run the following command to remove the **krb5-workstation** package:

```
# dnf remove krb5-workstation
```

**- OR -**

Run the following command to update the **krb5-workstation** package if it is required and approved by local site policy:

```
# dnf update krb5-workstation
```

**References:**

- 1. NIST SP 800-53 :: IA-7
- 2. NIST SP 800-53A :: IA-7.1

**Additional Information:**

Red Hat Enterprise Linux 8

Red Hat Enterprise Linux 8 STIG  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024  
  
GROUP ID: V-230239  
RULE ID: SV-230239r646864  
STIG ID: RHEL-08-010162  
SEVERITY: CAT II

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | 4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | 9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## 2.3 Configure Time Synchronization

It is recommended that systems be configured to synchronize their time using a service such as **chrony**.

Virtual systems may be configured to receive their time synchronization from their host system.

The host system must be configured to synchronize its time from an authoritative source to be considered compliant with this section.

Any "physical" clock present on a system should be synchronized from an authoritative time source.

### **Only one time synchronization method should be in use on the system**

**Notes:** Only the section related to the time synchronization method in use on the system should be followed, all other time synchronization recommendations should be skipped

### 2.3.1 Ensure time synchronization is in use (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

System time should be synchronized between all systems in an environment. This is typically done by establishing an authoritative time server or set of servers and having all systems synchronize their clocks to them.

**Note:** If another method for time synchronization is being used, this section may be skipped.

#### Rationale:

Time synchronization is important to support time sensitive security mechanisms like Kerberos and also ensures log files have consistent time records across the enterprise, which aids in forensic investigations.

#### Audit:

Run the following commands to verify that **chrony** is installed:

```
# rpm -q chrony  
chrony-<version>
```

#### Remediation:

Run the following command to install **chrony**:

```
# dnf install chrony
```

#### References:

1. NIST SP 800-53 Rev. 5: AU-3, AU-12

#### Additional Information:

On systems where host based time synchronization is not available, verify that **chrony** is installed.

On systems where host based time synchronization is available consult your documentation and verify that host based synchronization is in use.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                      | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.4 <u>Standardize Time Synchronization</u></b><br>Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.                                                          |      | ●    | ●    |
| v7               | <b>6.1 <u>Utilize Three Synchronized Time Sources</u></b><br>Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent. |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1562, T1562.001 | TA0005  |             |

## 2.3.2 *Ensure chrony is configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

- server
  - The server directive specifies an NTP server which can be used as a time source. The client-server relationship is strictly hierarchical: a client might synchronize its system time to that of the server, but the server's system time will never be influenced by that of a client.
  - This directive can be used multiple times to specify multiple servers.
  - The directive is immediately followed by either the name of the server, or its IP address.
- pool
  - The syntax of this directive is similar to that for the server directive, except that it is used to specify a pool of NTP servers rather than a single NTP server. The pool name is expected to resolve to multiple addresses which might change over time.
  - This directive can be used multiple times to specify multiple pools.
  - All options valid in the server directive can be used in this directive too.

### **Rationale:**

Time synchronization is important to support time sensitive security mechanisms and to ensure log files have consistent time records across the enterprise to aid in forensic investigations

## Audit:

Run the following script to ensure **chrony** is configured with an authorized timeserver:

```
#!/usr/bin/env bash

{
    a_output=() a_output2=() a_config_files=("/etc/chrony.conf")
    l_include='(confdir|sourcedir)' l_parameter_name='(server|pool)'
    l_parameter_value='.+ '
    while IFS= read -r l_conf_loc; do
        l_dir="" l_ext=""
        if [ -d "$l_conf_loc" ]; then
            l_dir="$l_conf_loc" l_ext=""
        elif grep -Psq '\/\*\.([^\#/\n\r]+)?\h*$' <<< "$l_conf_loc" || [ -f
"$$(readlink -f "$l_conf_loc")" ]; then
            l_dir="$(dirname "$l_conf_loc")" l_ext="$(basename "$l_conf_loc")"
        fi
        if [[ -n "$l_dir" && -n "$l_ext" ]]; then
            while IFS= read -r -d $'\0' l_file_name; do
                [ -f "$(readlink -f "$l_file_name")" ] &&
a_config_files+=("$$(readlink -f "$l_file_name")")
                done < <(find -L "$l_dir" -type f -name "$l_ext" -print0
2>/dev/null)
            fi
            done < <(awk 'l~/^\s*'"$l_include"'$/{print $2}' "${a_config_files[*]}")
2>/dev/null)
            for l_file in "${a_config_files[@]}"; do
                l_parameter_line="$(grep -Psi
'^\h*'"$l_parameter_name"'(\h+|\h*:\h*)'"$l_parameter_value"' \b' "$l_file")"
                [ -n "$l_parameter_line" ] && a_output+=(" - Parameter: \"$(tr -d '()'
<<< ${l_parameter_name//|/ or })\" \" \" \
                "      Exists in the file: \"$l_file\" as: \" $l_parameter_line")
            done
            [ "${#a_output[@]}" -le 0 ] && a_output2+=(" - Parameter: \"$(tr -d
'()' <<< ${l_parameter_name//|/ or })\" \" \" \
            "      Does not exist in the chrony configuration")
            if [ "${#a_output2[@]}" -le 0 ]; then
                printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
            else
                printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
            fi
        fi
    }
}
```

## Remediation:

Edit `/etc/chrony.conf` or a file ending in `.sources` in `/etc/sources.d/` and add or edit server or pool lines as appropriate according to local site policy:

Edit the **Chrony** configuration and add or edit the server and/or pool lines returned by the Audit Procedure as appropriate according to local site policy

```
<[server|pool]> <[remote-server|remote-pool]>
```

*Example script to add a drop-in configuration for the **pool** directive:*

```
#!/usr/bin/env bash

{
    [ ! -d "/etc/sources.d/" ] && mkdir /etc/sources.d/
    printf '%s\n' "" "#The maxsources option is unique to the pool directive" \
    "pool time.nist.gov iburst maxsources 4" >> /etc/sources.d/60-
sources.sources
    chronyc reload sources &>/dev/null
}
```

*Example script to add a drop-in configuration for the **server** directive:*

```
#!/usr/bin/env bash

{
    [ ! -d "/etc/sources.d/" ] && mkdir /etc/sources.d/
    printf '%s\n' "" "server time-a-g.nist.gov iburst" "server 132.163.97.3
iburst" \
    "server time-d-b.nist.gov iburst" >> /etc/sources.d/60-sources.sources
    chronyc reload sources &>/dev/null
}
```

Run the following command to reload the **chronyd** config:

```
# systemctl reload-or-restart chronyd
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3, AU-12

## Additional Information:

On systems where host based time synchronization is not available, verify that **chrony** is installed.

On systems where host based time synchronization is available consult your documentation and verify that host based synchronization is in use.



### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                      | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.4 <u>Standardize Time Synchronization</u></b><br>Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.                                                          |      |  |  |
| v7               | <b>6.1 <u>Utilize Three Synchronized Time Sources</u></b><br>Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent. |      |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1070, T1070.002            | TA0002  | M1022       |

### 2.3.3 Ensure chrony is not run as the root user (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The file `/etc/sysconfig/chronyd` allows configuration of options for `chrony` to include the user `chrony` is run as. By default, this is set to the user `chrony`

#### Rationale:

Services should not be set to run as the root user

#### Audit:

Run the following command to verify that `chrony` isn't configured to run as the `root` user:

```
# grep -Psi -- '^h*OPTIONS=\"?\h*([^\n\r]+\h+)?-u\h+root\b'
/etc/sysconfig/chronyd

Nothing should be returned
```

#### Remediation:

Edit the file `/etc/sysconfig/chronyd` and add or modify the following line to remove `"-u root"` from any `OPTIONS=` argument:

*Example:*

```
OPTIONS="-F 2"
```

Run the following command to reload the `chronyd.service` configuration:

```
# systemctl reload-or-restart chronyd.service
```

#### Default Value:

```
OPTIONS="-F 2"
```

### *2.3.4 Ensure the operating system is securely comparing internal information system clocks at least every 24 hours with an NTP server (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

must securely compare internal information system clocks at least every 24 hours with a server synchronized to an authoritative time source, such as the United States Naval Observatory (USNO) time servers, or a time server designated for the appropriate DoD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).

#### **Rationale:**

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

Organizations should consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

If time stamps are not consistently applied and there is no common time reference, it is difficult to perform forensic analysis.

Time stamps generated by the operating system include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

RHEL 8 operating systems utilize the "timedatectl" command to view the status of the "systemd-timesyncd.service". The "timedatectl" status will display the local time, UTC, and the offset from UTC.

Note that USNO offers authenticated NTP service to DoD and U.S. Government agencies operating on the NIPR and SIPR networks. Visit <https://www.usno.navy.mil/USNO/time/ntp/dod-customers> for more information.

Satisfies: SRG-OS-000355-GPOS-00143, SRG-OS-000356-GPOS-00144, SRG-OS-000359-GPOS-00146

## Audit:

Verify the operating system is securely comparing internal information system clocks at least every 24 hours with an NTP server with the following commands:

```
# grep maxpoll /etc/chrony.conf  
  
server 0.us.pool.ntp.mil iburst maxpoll 16
```

If the "maxpoll" option is set to a number greater than 16 or the line is commented out, this is a finding.

Verify the "chrony.conf" file is configured to an authoritative DoD time source by running the following command:

```
# grep -i server /etc/chrony.conf  
server 0.us.pool.ntp.mil
```

If the parameter "server" is not set or is not set to an authoritative DoD time source, this is a finding.

## Remediation:

Configure the operating system to securely compare internal information system clocks at least every 24 hours with an NTP server by adding/modifying the following line in the /etc/chrony.conf file.

```
server [ntp.server.name] iburst maxpoll 16
```

## References:

1. NIST SP 800-53 Revision 4 :: AU-8 (1) (a)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230484  
Rule ID: SV-230484r877038  
STIG ID: RHEL-08-030740  
Severity: CAT II

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                      | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.4 <u>Standardize Time Synchronization</u></b><br>Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.                                                          |      |  |  |
| v7               | <b>6.1 <u>Utilize Three Synchronized Time Sources</u></b><br>Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent. |      |  |  |

### 2.3.5 Ensure the operating system disables network management of the chrony daemon (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must disable network management of the chrony daemon.

#### Rationale:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Not exposing the management interface of the chrony daemon on the network diminishes the attack space.

RHEL 8 operating systems utilize the "timedatectl" command to view the status of the "systemd-timesyncd.service". The "timedatectl" status will display the local time, UTC, and the offset from UTC.

Note that USNO offers authenticated NTP service to DoD and U.S. Government agencies operating on the NIPR and SIPR networks. Visit <https://www.usno.navy.mil/USNO/time/ntp/dod-customers> for more information.

#### Audit:

Verify the operating system disables network management of the chrony daemon with the following command:

```
# grep -w 'cmdport' /etc/chrony.conf  
  
cmdport 0
```

If the "cmdport" option is not set to "0", is commented out or missing, this is a finding.

#### Remediation:

Configure the operating system disable network management of the chrony daemon by adding/modifying the following line in the /etc/chrony.conf file.

```
cmdport 0
```

#### References:

1. NIST SP 800-53 Revision 5 :: CM-7 a
2. NIST SP 800-53A :: CM-7.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230486  
Rule ID: SV-230486r928593  
STIG ID: RHEL-08-030742  
Severity: CAT III

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

### *2.3.6 Ensure the operating system disables the chrony daemon from acting as a server (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must disable the chrony daemon from acting as a server.

#### **Rationale:**

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Minimizing the exposure of the server functionality of the chrony daemon diminishes the attack surface.

RHEL 8 operating systems utilize the "timedatectl" command to view the status of the "systemd-timesyncd.service". The "timedatectl" status will display the local time, UTC, and the offset from UTC.

Note that USNO offers authenticated NTP service to DoD and U.S. Government agencies operating on the NIPR and SIPR networks. Visit <https://www.usno.navy.mil/USNO/time/ntp/dod-customers> for more information.

#### **Audit:**

Verify the operating system disables the chrony daemon from acting as a server with the following command:

```
# grep -w 'port' /etc/chrony.conf  
port 0
```

If the "port" option is not set to "0", is commented out or missing, this is a finding.

#### **Remediation:**

Configure the operating system to disable the chrony daemon from acting as a server by adding/modifying the following line in the "/etc/chrony.conf" file.

```
port 0
```

#### **References:**

1. NIST SP 800-53 Revision 5 :: CM-7 a
2. NIST SP 800-53A :: CM-7.1 (ii)



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230485  
Rule ID: SV-230485r928590  
STIG ID: RHEL-08-030741  
Severity: CAT III

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## 2.4 Job Schedulers

A job scheduler is used to execute jobs, commands, or shell scripts, at fixed times, dates, or intervals

## 2.4.1 Configure cron

**cron** is a time based job scheduler

- **IF** - **cron** is not installed on the system, this sub section can be skipped

**Note:** Other methods such as **systemd timers** exist for scheduling jobs. If another method is used **cron** should may be removed. The alternate method should be secured in accordance with local site policy

### 2.4.1.1 Ensure cron daemon is enabled and active (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The **cron** daemon is used to execute batch jobs on the system.

#### Rationale:

While there may not be user jobs that need to be run on the system, the system does have maintenance jobs that may include security monitoring that have to run, and **cron** is used to execute them.

#### Audit:

- **IF** - cron is installed on the system:

Run the following command to verify **cron** is enabled:

```
# systemctl list-unit-files | awk '$1~/^crond?\.service/{print $2}'  
  
enabled
```

Run the following command to verify that **cron** is active:

```
# systemctl list-units | awk '$1~/^crond?\.service/{print $3}'  
  
active
```

#### Remediation:

- **IF** - cron is installed on the system:

Run the following commands to unmask, enable, and start **cron**:

```
# systemctl unmask "$(systemctl list-unit-files | awk  
'$1~/^crond?\.service/{print $1}')" "  
# systemctl --now enable "$(systemctl list-unit-files | awk  
'$1~/^crond?\.service/{print $1}')" "
```

#### References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1562, T1562.001                   | TA0005         | M1018              |

### 2.4.1.2 Ensure permissions on /etc/crontab are configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The `/etc/crontab` file is used by `cron` to control its own jobs. The commands in this item make sure that root is the user and group owner of the file and that only the owner can access the file.

#### Rationale:

This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

#### Audit:

- **IF** - cron is installed on the system:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other` :

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/crontab
Access: (600/-rw-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

#### Remediation:

- **IF** - cron is installed on the system:

Run the following commands to set ownership and permissions on `/etc/crontab`:

```
# chown root:root /etc/crontab
# chmod og-rwx /etc/crontab
```

#### Default Value:

Access: (644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)

#### References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics        | Mitigations |
|-----------------------------|----------------|-------------|
| T1053, T1053.003            | TA0002, TA0007 | M1018       |

### 2.4.1.3 Ensure permissions on /etc/cron.hourly are configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

This directory contains system **cron** jobs that need to run on an hourly basis. The files in this directory cannot be manipulated by the **crontab** command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

#### Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

#### Audit:

- **IF** - cron is installed on the system:

Run the following command and verify **Uid** and **Gid** are both **0/root** and **Access** does not grant permissions to **group** or **other**:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.hourly/  
Access: (700/drwx-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

#### Remediation:

- **IF** - cron is installed on the system:

Run the following commands to set ownership and permissions on the **/etc/cron.hourly** directory:

```
# chown root:root /etc/cron.hourly/  
# chmod og-rwx /etc/cron.hourly/
```

#### Default Value:

Access: (755/drwxr-xr-x) Uid: ( 0/ root) Gid: ( 0/ root)

#### References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2



## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics        | Mitigations |
|-----------------------------|----------------|-------------|
| T1053, T1053.003            | TA0002, TA0007 | M1018       |

#### 2.4.1.4 Ensure permissions on /etc/cron.daily are configured (Automated)

##### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

##### Description:

The `/etc/cron.daily` directory contains system cron jobs that need to run on a daily basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

##### Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

##### Audit:

- **IF** - cron is installed on the system:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.daily/  
Access: (700/drwx-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

##### Remediation:

- **IF** - cron is installed on the system:

Run the following commands to set ownership and permissions on the `/etc/cron.daily` directory:

```
# chown root:root /etc/cron.daily/  
# chmod og-rwx /etc/cron.daily/
```

##### Default Value:

Access: (755/drwxr-xr-x) Uid: ( 0/ root) Gid: ( 0/ root)

##### References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics        | Mitigations |
|-----------------------------|----------------|-------------|
| T1053, T1053.003            | TA0002, TA0007 | M1018       |

### 2.4.1.5 Ensure permissions on /etc/cron.weekly are configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The `/etc/cron.weekly` directory contains system cron jobs that need to run on a weekly basis. The files in this directory cannot be manipulated by the `crontab` command but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

#### Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

#### Audit:

- **IF** - cron is installed on the system:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.weekly/  
Access: (700/drwx-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

#### Remediation:

- **IF** - cron is installed on the system:

Run the following commands to set ownership and permissions on the `/etc/cron.weekly` directory:

```
# chown root:root /etc/cron.weekly/  
# chmod og-rwx /etc/cron.weekly/
```

#### Default Value:

Access: (755/drwxr-xr-x) Uid: ( 0/ root) Gid: ( 0/ root)

#### References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics        | Mitigations |
|-----------------------------|----------------|-------------|
| T1053, T1053.003            | TA0002, TA0007 | M1018       |

## 2.4.1.6 Ensure permissions on /etc/cron.monthly are configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The `/etc/cron.monthly` directory contains system cron jobs that need to run on a monthly basis. The files in this directory cannot be manipulated by the `crontab` command but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

### Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

### Audit:

- **IF** - cron is installed on the system:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.monthly/  
Access: (700/drwx-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

### Remediation:

- **IF** - cron is installed on the system:

Run the following commands to set ownership and permissions on the `/etc/cron.monthly` directory:

```
# chown root:root /etc/cron.monthly/  
# chmod og-rwx /etc/cron.monthly/
```

### Default Value:

Access: (755/drwxr-xr-x) Uid: ( 0/ root) Gid: ( 0/ root)

### References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics        | Mitigations |
|-----------------------------|----------------|-------------|
| T1053, T1053.003            | TA0002, TA0007 | M1018       |

### 2.4.1.7 Ensure permissions on /etc/cron.d are configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The `/etc/cron.d` directory contains system `cron` jobs that need to run in a similar manner to the hourly, daily weekly and monthly jobs from `/etc/crontab`, but require more granular control as to when they run. The files in this directory cannot be manipulated by the `crontab` command but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

#### Rationale:

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

#### Audit:

- **IF** - cron is installed on the system:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat -Lc 'Access: (%a/%A) Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/cron.d/  
Access: (700/drwx-----) Uid: ( 0/ root) Gid: ( 0/ root)
```

#### Remediation:

- **IF** - cron is installed on the system:

Run the following commands to set ownership and permissions on the `/etc/cron.d` directory:

```
# chown root:root /etc/cron.d/  
# chmod og-rwx /etc/cron.d/
```

#### Default Value:

Access: (755/drwxr-xr-x) Uid: ( 0/ root) Gid: ( 0/ root)



## References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics        | Mitigations |
|-----------------------------|----------------|-------------|
| T1053, T1053.003            | TA0002, TA0007 | M1018       |

### 2.4.1.8 Ensure crontab is restricted to authorized users (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

**crontab** is the program used to install, deinstall, or list the tables used to drive the cron daemon. Each user can have their own crontab, and though these are files in **/var/spool/cron/crontabs**, they are not intended to be edited directly.

If the **/etc/cron.allow** file exists, then you must be listed (one user per line) therein in order to be allowed to use this command. If the **/etc/cron.allow** file does not exist but the **/etc/cron.deny** file does exist, then you must not be listed in the **/etc/cron.deny** file in order to use this command.

If neither of these files exists, then depending on site-dependent configuration parameters, only the super user will be allowed to use this command, or all users will be able to use this command.

If both files exist then **/etc/cron.allow** takes precedence. Which means that **/etc/cron.deny** is not considered and your user must be listed in **/etc/cron.allow** in order to be able to use the crontab.

Regardless of the existence of any of these files, the root administrative user is always allowed to setup a crontab.

The files **/etc/cron.allow** and **/etc/cron.deny**, if they exist, must be either world-readable, or readable by group **crontab**. If they are not, then cron will deny access to all users until the permissions are fixed.

There is one file for each user's crontab under the **/var/spool/cron/crontabs** directory. Users are not allowed to edit the files under that directory directly to ensure that only users allowed by the system to run periodic tasks can add them, and only syntactically correct crontabs will be written there. This is enforced by having the directory writable only by the **crontab** group and configuring crontab command with the setgid bit set for that specific group.

#### Note:

- Even though a given user is not listed in **cron.allow**, cron jobs can still be run as that user
- The files **/etc/cron.allow** and **/etc/cron.deny**, if they exist, only controls administrative access to the crontab command for scheduling and modifying cron jobs

## Rationale:

On many systems, only the system administrator is authorized to schedule **cron** jobs. Using the **cron.allow** file to control who can run **cron** jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

## Audit:

- **IF** - cron is installed on the system:

Run the following command to verify **/etc/cron.allow**:

- Exists
- Is mode **0640** or more restrictive
- Is owned by the user **root**
- Is group owned by the group **root** - **OR** - the group **crontab**

```
# stat -Lc 'Access: (%a/%A) Owner: (%U) Group: (%G)' /etc/cron.allow
```

Verify the returned value is:

```
Access: (640/-rw-r-----) Owner: (root) Group: (root)
- OR -
Access: (640/-rw-r-----) Owner: (root) Group: (crontab)
```

Run the following command to verify either **cron.deny** doesn't exist or is:

- Mode **0640** or more restrictive
- Owned by the user **root**
- Is group owned by the group **root** - **OR** - the group **crontab**

```
# [ -e "/etc/cron.deny" ] && stat -Lc 'Access: (%a/%A) Owner: (%U) Group: (%G)' /etc/cron.deny
```

Verify either nothing is returned - **OR** - returned value is one of the following:

```
Access: (640/-rw-r-----) Owner: (root) Group: (root)
- OR -
Access: (640/-rw-r-----) Owner: (root) Group: (crontab)
```

**Note:** On systems where cron is configured to use the group **crontab**, if the group **crontab** is not set as the owner of **cron.allow**, then cron will deny access to all users and you will see an error similar to:

```
You (<USERNAME>) are not allowed to use this program (crontab)
See crontab(1) for more information
```

## Remediation:

- **IF** - cron is installed on the system:

Run the following script to:

- Create `/etc/cron.allow` if it doesn't exist
- Change owner to user `root`
- Change group owner to group `root` - **OR** - group `crontab` if it exists
- Change mode to `640` or more restrictive

```
#!/usr/bin/env bash

{
  [ ! -e "/etc/cron.allow" ] && touch /etc/cron.allow
  chmod u-x,g-wx,o-rwx /etc/cron.allow
  if grep -Pq -- '^\h*crontab\: ' /etc/group; then
    chown root:crontab /etc/cron.allow
  else
    chown root:root /etc/cron.allow
  fi
}
```

- **IF** - `/etc/cron.deny` exists, run the following script to:

- Change owner to user `root`
- Change group owner to group `root` - **OR** - group `crontab` if it exists
- Change mode to `640` or more restrictive

```
#!/usr/bin/env bash

{
  if [ -e "/etc/cron.deny" ]; then
    chmod u-x,g-wx,o-rwx /etc/cron.deny
    if grep -Pq -- '^\h*crontab\: ' /etc/group; then
      chown root:crontab /etc/cron.deny
    else
      chown root:root /etc/cron.deny
    fi
  fi
}
```

**Note:** On systems where cron is configured to use the group `crontab`, if the group `crontab` is not set as the owner of `cron.allow`, then cron will deny access to all users and you will see an error similar to:

```
You (<USERNAME>) are not allowed to use this program (crontab)
See crontab(1) for more information
```

## References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1053, T1053.003            | TA0002  | M1018       |

## 2.4.2 Configure at

**at** is a command-line utility used to schedule a job for later execution

**Note:** if **at** is not installed on the system, this section can be skipped

### 2.4.2.1 Ensure at is restricted to authorized users (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

**at** allows fairly complex time specifications, extending the POSIX.2 standard. It accepts times of the form HH:MM to run a job at a specific time of day. (If that time is already past, the next day is assumed.) You may also specify midnight, noon, or teatime (4pm) and you can have a time-of-day suffixed with AM or PM for running in the morning or the evening. You can also say what day the job will be run, by giving a date in the form month-name day with an optional year, or giving a date of the form MMDD[CC]YY, MM/DD/[CC]YY, DD.MM.[CC]YY or [CC]YY-MM-DD. The specification of a date must follow the specification of the time of day. You can also give times like now + count time-units, where the time-units can be minutes, hours, days, or weeks and you can tell at to run the job today by suffixing the time with today and to run the job tomorrow by suffixing the time with tomorrow.

The **/etc/at.allow** and **/etc/at.deny** files determine which user can submit commands for later execution via at or batch. The format of the files is a list of usernames, one on each line. Whitespace is not permitted. If the file **/etc/at.allow** exists, only usernames mentioned in it are allowed to use at. If **/etc/at.allow** does not exist, **/etc/at.deny** is checked, every username not mentioned in it is then allowed to use at. An empty **/etc/at.deny** means that every user may use at. If neither file exists, only the superuser is allowed to use at.

#### Rationale:

On many systems, only the system administrator is authorized to schedule **at** jobs. Using the **at.allow** file to control who can run **at** jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

## Audit:

- **IF** - at is installed on the system:

Run the following command to verify `/etc/at.allow`:

- Exists
- Is mode `0640` or more restrictive
- Is owned by the user `root`
- Is group owned by the group `daemon` or group `root`

```
# stat -Lc 'Access: (%a/%A) Owner: (%U) Group: (%G)' /etc/at.allow
Access: (640/-rw-r-----) Owner: (root) Group: (daemon)
-OR-
Access: (640/-rw-r-----) Owner: (root) Group: (root)
```

Verify mode is `640` or more restrictive, owner is `root`, and group is `daemon` or `root`

Run the following command to verify `at.deny` doesn't exist, **-OR-** is:

- Mode `0640` or more restrictive
- Owned by the user `root`
- Group owned by the group `daemon` or group `root`

```
# [ -e "/etc/at.deny" ] && stat -Lc 'Access: (%a/%A) Owner: (%U) Group: (%G)' /etc/at.deny
Access: (640/-rw-r-----) Owner: (root) Group: (daemon)
-OR-
Access: (640/-rw-r-----) Owner: (root) Group: (root)
-OR-
Nothing is returned
```

If a value is returned, verify mode is `640` or more restrictive, owner is `root`, and group is `daemon` or `root`



## Remediation:

- **IF** - at is installed on the system:  
Run the following script to:

- **/etc/at.allow:**
  - Create the file if it doesn't exist
  - Change owner or user **root**
  - If group **daemon** exists, change to group **daemon**, else change group to **root**
  - Change mode to **640** or more restrictive
- - **IF** - **/etc/at.deny** exists:
  - Change owner or user **root**
  - If group **daemon** exists, change to group **daemon**, else change group to **root**
  - Change mode to **640** or more restrictive

```
#!/usr/bin/env bash

{
  grep -Pq -- '^daemon\b' /etc/group && l_group="daemon" || l_group="root"
  [ ! -e "/etc/at.allow" ] && touch /etc/at.allow
  chown root:$l_group /etc/at.allow
  chmod u-x,g-wx,o-rwx /etc/at.allow
  [ -e "/etc/at.deny" ] && chown root:$l_group /etc/at.deny
  [ -e "/etc/at.deny" ] && chmod u-x,g-wx,o-rwx /etc/at.deny
}
```

## References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1053, T1053.003                   | TA0002         | M1018              |

## 2.5 Configure USBGuard

The USBGuard-daemon is the main component of the USBGuard software framework. It runs as a service in the background and enforces the USB device authorization policy for all USB devices

## 2.5.1 Ensure USBGuard is installed on the operating system (Automated)

### Profile Applicability:

- STIG

### Description:

The operating system must have USBGuard installed.

### Rationale:

Without authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity.

Peripherals include, but are not limited to, such devices as flash drives, external storage, and printers.

A new feature that RHEL 8 operating systems provide is the USBGuard software framework. The USBguard-daemon is the main component of the USBGuard software framework. It runs as a service in the background and enforces the USB device authorization policy for all USB devices. The policy is defined by a set of rules using a rule language described in the "usbguard-rules.conf" file. The policy and the authorization state of USB devices can be modified during runtime using the USBGuard tool.

The System Administrator (SA) must work with the site Information System Security Officer (ISSO) to determine a list of authorized peripherals and establish rules within the USBGuard software framework to allow only authorized devices.

### Audit:

Verify USBGuard is installed on the operating system with the following command:

```
# dnf list installed usbguard

Installed Packages
usbguard.x86_64 0.7.8-7.el8 @ol8_appstream
```

If the USBGuard package is not installed, ask the SA to indicate how unauthorized peripherals are being blocked.

If there is no evidence that unauthorized peripherals are being blocked before establishing a connection, this is a finding.

## Remediation:

Install the USBGuard package with the following command:

```
# dnf install usbguard.x86_64
```

## References:

1. NIST SP 800-53 Revision 5 :: IA-3

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244547  
Rule ID: SV-244547r854076  
STIG ID: RHEL-08-040139  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.1 Establish and Maintain a Secure Configuration Process</b><br>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |
| v7               | <b>13.7 Manage USB Devices</b><br>If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.                                                                                                                                                                                         |                                                                                       |  |  |

## 2.5.2 Ensure USBGuard has a policy configured (Manual)

### Profile Applicability:

- STIG

### Description:

The operating system must block unauthorized peripherals before establishing a connection.

### Rationale:

Without authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity.

Peripherals include, but are not limited to, such devices as flash drives, external storage, and printers.

A new feature that RHEL 8 operating system's provide is the USBGuard software framework. The USBGuard-daemon is the main component of the USBGuard software framework. It runs as a service in the background and enforces the USB device authorization policy for all USB devices. The policy is defined by a set of rules using a rule language described in the usbguard-rules.conf file. The policy and the authorization state of USB devices can be modified during runtime using the USBGuard tool.

The System Administrator (SA) must work with the site Information System Security Officer (ISSO) to determine a list of authorized peripherals and establish rules within the USBGuard software framework to allow only authorized devices.

### Audit:

Verify the USBGuard has a policy configured with the following command:

```
# usbguard list-rules
```

If the command does not return results or an error is returned, ask the SA to indicate how unauthorized peripherals are being blocked.

If there is no evidence that unauthorized peripherals are being blocked before establishing a connection, this is a finding.

Remediation:

Configure the operating system to enable the blocking of unauthorized peripherals with the following command:  
This command must be run from a root shell and will create an allow list for any USB devices currently connect to the system.

```
# usbguard generate-policy > /etc/usbguard/rules.conf
```

Note: Enabling and starting USBguard without properly configuring it for an individual system will immediately prevent any access over a USB device such as a keyboard or mouse

References:

- 1. NIST SP 800-53 Revision 5 :: IA-3

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230524  
Rule ID: SV-230524r854065  
STIG ID: RHEL-08-040140  
Severity: CAT II

CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                       | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped                                                                                                                                                                     |      |                                                                                       |                                                                                       |
| v7               | 13.7 <u>Manage USB Devices</u><br>If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained. |      |  |  |

### *2.5.3 Ensure the operating system enables Linux audit logging of the USBGuard daemon (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must enable Linux audit logging for the USBGuard daemon.

#### **Rationale:**

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

If auditing is enabled late in the startup process, the actions of some startup processes may not be audited. Some audit systems also maintain state information only available if auditing is enabled before a given process is created.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records.

DoD has defined the list of events for which the operating system will provide an audit record generation capability as the following:

1. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels);
2. Access actions, such as successful and unsuccessful logon attempts, privileged activities or other system-level access, starting and ending time for user access to the system, concurrent logons from different workstations, successful and unsuccessful accesses to objects, all program initiations, and all direct access to the information system;
3. All account creations, modifications, disabling, and terminations; and
4. All kernel module load, unload, and restart actions.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000471-GPOS-00215



## Audit:

Verify the operating system enables Linux audit logging of the USBGuard daemon with the following commands:

Note: If the USBGuard daemon is not installed and enabled, this requirement is not applicable.

```
# grep -i auditbackend /etc/usbguard/usbguard-daemon.conf  
  
AuditBackend=LinuxAudit
```

If the "AuditBackend" entry does not equal "LinuxAudit", is missing, or the line is commented out, this is a finding.

## Remediation:

Configure the operating system to enable Linux audit logging of the USBGuard daemon by adding or modifying the following line in "/etc/usbguard/usbguard-daemon.conf":

```
AuditBackend=LinuxAudit
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

```
Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024  
  
Vul ID: V-230470  
Rule ID: SV-230470r744006  
STIG ID: RHEL-08-030603  
Severity: CAT III
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

## 2.5.4 Ensure the usbguard service is enabled and active (Automated)

### Profile Applicability:

- STIG

### Description:

The operating system must enable USBGuard.

### Rationale:

Without authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity.

Peripherals include, but are not limited to, such devices as flash drives, external storage, and printers.

A new feature that RHEL 8 operating systems provide is the USBGuard software framework. The USBGuard-daemon is the main component of the USBGuard software framework. It runs as a service in the background and enforces the USB device authorization policy for all USB devices. The policy is defined by a set of rules using a rule language described in the "usbguard-rules.conf" file. The policy and the authorization state of USB devices can be modified during runtime using the USBGuard tool.

The System Administrator (SA) must work with the site Information System Security Officer (ISSO) to determine a list of authorized peripherals and establish rules within the USBGuard software framework to allow only authorized devices.

### Audit:

Verify the operating system has enabled the use of the USBGuard with the following command:

```
# systemctl status usbguard.service

usbguard.service - USBGuard daemon
Loaded: loaded (/usr/lib/systemd/system/usbguard.service; enabled; vendor
preset: disabled)
Active: active (running)
```

If the usbguard.service is not enabled and active, ask the SA to indicate how unauthorized peripherals are being blocked.

If there is no evidence that unauthorized peripherals are being blocked before establishing a connection, this is a finding.

**Remediation:**

Configure the operating system to enable the blocking of unauthorized peripherals with the following commands:

```
# systemctl enable usbguard.service
# systemctl start usbguard.service
```

Note: Enabling and starting USBGuard without properly configuring it for an individual system will immediately prevent any access over a USB device such as a keyboard or mouse.

**References:**

- 1. NIST SP 800-53 Revision 5 :: IA-3

**Additional Information:**

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244548

Rule ID: SV-244548r854077

STIG ID: RHEL-08-040141

Severity: CAT II

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                       | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped                                                                                                                                                                     |      |                                                                                       |                                                                                       |
| v7               | 13.7 <u>Manage USB Devices</u><br>If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained. |      |  |  |

## 2.6 Configure fapolicyd

The **fapolicyd** software framework controls the execution of applications based on a user-defined policy. This is one of the most efficient ways to prevent running untrusted and possibly malicious applications on the system

## 2.6.1 Ensure fapolicyd is installed (Automated)

### Profile Applicability:

- STIG

### Description:

The "fapolicy" module must be installed.

### Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

Utilizing a whitelist provides a configuration management method for allowing the execution of only authorized software. Using only authorized software decreases risk by limiting the number of potential vulnerabilities. Verification of whitelisted software occurs prior to execution or at system startup.

User home directories/folders may contain information of a sensitive nature. Non-privileged users should coordinate any sharing of information with an SA through shared resources.

RHEL 8 operating system's ship with many optional packages. One such package is a file access policy daemon called "fapolicyd". "fapolicyd" is a userspace daemon that determines access rights to files based on attributes of the process and file. It can be used to either blacklist or whitelist processes or file access.

Proceed with caution with enforcing the use of this daemon. Improper configuration may render the system non-functional. The "fapolicyd" API is not namespace aware and can cause issues when launching or running containers.

Satisfies: SRG-OS-000368-GPOS-00154, SRG-OS-000370-GPOS-00155, SRG-OS-000480-GPOS-00232

### Audit:

Verify that "fapolicyd" is installed.

Check that "fapolicyd" is installed with the following command:

```
# dnf list installed fapolicyd

Installed Packages
fapolicyd.x86_64
```

If fapolicyd is not installed, this is a finding.

## Remediation:

Install "fapolicyd" with the following command:

```
# dnf install fapolicyd.x86_64
```

## References:

1. NIST SP 800-53 Revision 5 :: CM-7 (2)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230523  
Rule ID: SV-230523r854064  
STIG ID: RHEL-08-040135  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

## *2.6.2 Ensure fapolicyd employs a deny-all, permit-by-exception policy (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

The "fapolicy" module must be configured to employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs.

### **Rationale:**

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

Utilizing a whitelist provides a configuration management method for allowing the execution of only authorized software. Using only authorized software decreases risk by limiting the number of potential vulnerabilities. Verification of whitelisted software occurs prior to execution or at system startup.

User home directories/folders may contain information of a sensitive nature. Non-privileged users should coordinate any sharing of information with an SA through shared resources.

RHEL 8 operating systems ship with many optional packages. One such package is a file access policy daemon called "fapolicyd". "fapolicyd" is a userspace daemon that determines access rights to files based on attributes of the process and file. It can be used to either blacklist or whitelist processes or file access.

Proceed with caution with enforcing the use of this daemon. Improper configuration may render the system non-functional. The "fapolicyd" API is not namespace aware and can cause issues when launching or running containers.

Satisfies: SRG-OS-000368-GPOS-00154, SRG-OS-000370-GPOS-00155, SRG-OS-000480-GPOS-00232

## Audit:

Verify the operating system's "fapolicyd" employs a deny-all, permit-by-exception policy. Check that "fapolicyd" is in enforcement mode with the following command:

```
# grep permissive /etc/fapolicyd/fapolicyd.conf  
permissive = 0
```

Check that "fapolicyd" employs a deny-all policy on system mounts with the following commands:

```
# tail /etc/fapolicyd/fapolicyd.rules  
  
allow exe=/usr/bin/python3.7 : ftype=text/x-python  
deny_audit perm=any pattern=ld_so : all  
deny perm=any all : all  
  
# cat /etc/fapolicyd/fapolicyd.mounts  
  
/dev/shm  
/run  
/sys/fs/cgroup  
/  
/home  
/boot  
/run/user/42  
/run/user/1000
```

If "fapolicyd" is not running in enforcement mode on all system mounts with a deny-all, permit-by-exception policy, this is a finding.



## Remediation:

Configure the operating system to employ a deny-all, permit-by-exception application whitelisting policy with "fapolicyd" using the following command:

Note: Running this command requires a root shell

```
# mount | egrep '^tmpfs| ext4| ext3| xfs' | awk '{ printf "%s\n", $3 }' >> /etc/fapolicyd/fapolicyd.mounts
```

With the "fapolicyd" installed and enabled, configure the daemon to function in permissive mode until the whitelist is built correctly to avoid system lockout. Do this by editing the "/etc/fapolicyd/fapolicyd.conf" file with the following line:

```
permissive = 1
```

Build the whitelist in the "/etc/fapolicyd/fapolicyd.rules" file ensuring the last rule is "deny perm=any all : all".

Once it is determined the whitelist is built correctly, set fapolicyd to enforcing mode by editing the "permissive" line in the "/etc/fapolicyd/fapolicyd.conf" file.

```
permissive = 0
```

## References:

1. NIST SP 800-53 Revision 5 :: CM-7 (2)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244546  
Rule ID: SV-244546r858730  
STIG ID: RHEL-08-040137  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                             | IG 1 | IG 2 | IG 3 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>2.5 Allowlist Authorized Software</b><br>Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently. |      | ●    | ●    |
| v7               | <b>2.6 Address unapproved software</b><br>Ensure that unauthorized software is either removed or the inventory is updated in a timely manner                                                                        | ●    | ●    | ●    |

### 2.6.3 Ensure fapolicyd is enabled and running (Automated)

#### Profile Applicability:

- STIG

#### Description:

The "fapolicyd" module must be enabled.

#### Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting or more correctly allow listing.

Utilizing a whitelist provides a configuration management method for allowing the execution of only authorized software. Using only authorized software decreases risk by limiting the number of potential vulnerabilities. Verification of whitelisted software occurs prior to execution or at system startup.

User home directories/folders may contain information of a sensitive nature. Non-privileged users should coordinate any sharing of information with an SA through shared resources.

RHEL 8 operating systems ship with many optional packages. One such package is a file access policy daemon called "fapolicyd". "fapolicyd" is a userspace daemon that determines access rights to files based on attributes of the process and file. It can be used to either blacklist or whitelist processes or file access.

Proceed with caution with enforcing the use of this daemon. Improper configuration may render the system non-functional. The "fapolicyd" API is not namespace aware and can cause issues when launching or running containers.

Satisfies: SRG-OS-000368-GPOS-00154, SRG-OS-000370-GPOS-00155, SRG-OS-000480-GPOS-00232

#### Audit:

Verify "fapolicyd" is enabled and running with the following command:

```
# systemctl status fapolicyd.service

fapolicyd.service - File Access Policy Daemon
Loaded: loaded (/usr/lib/systemd/system/fapolicyd.service; enabled; vendor
preset: disabled)
Active: active (running)
```

If fapolicyd is not enabled and running, this is a finding.

**Remediation:**

Enable "fapolicyd" using the following command:

```
# systemctl enable --now fapolicyd
```

**References:**

- 1. NIST SP 800-53 Revision 5 :: CM-7 (2)

**Additional Information:**

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244545

Rule ID: SV-244545r854074

STIG ID: RHEL-08-040136

Severity: CAT II

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                             | IG 1 | IG 2 | IG 3 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <u>2.5 Allowlist Authorized Software</u><br>Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently. |      |      |      |
| v7               | <u>2.6 Address unapproved software</u><br>Ensure that unauthorized software is either removed or the inventory is updated in a timely manner                                                                        |      |      |      |

## 3 Network

This section provides guidance on for securing the network configuration of the system

## 3.1 Configure Network Devices

To reduce the attack surface of a system, unused devices should be disabled.

**Note:** This should not be considered a comprehensive list, you may wish to consider additions to those listed here for your environment.

### *3.1.1 Ensure IPv6 status is identified (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Internet Protocol Version 6 (IPv6) is the most recent version of Internet Protocol (IP). It's designed to supply IP addressing and additional security to support the predicted growth of connected devices. IPv6 is based on 128-bit addressing and can support 340 undecillion, which is 340,282,366,920,938,463,374,607,431,768,211,456 unique addresses.

#### Features of IPv6

- Hierarchical addressing and routing infrastructure
- Stateful and Stateless configuration
- Support for quality of service (QoS)
- An ideal protocol for neighboring node interaction

#### **Rationale:**

IETF RFC 4038 recommends that applications are built with an assumption of dual stack. It is recommended that IPv6 be enabled and configured in accordance with Benchmark recommendations.

- **IF** - dual stack and IPv6 are not used in your environment, IPv6 may be disabled to reduce the attack surface of the system, and recommendations pertaining to IPv6 can be skipped.

**Note:** It is recommended that IPv6 be enabled and configured unless this is against local site policy

#### **Impact:**

IETF RFC 4038 recommends that applications are built with an assumption of dual stack.

When enabled, IPv6 will require additional configuration to reduce risk to the system.

## Audit:

Run the following script to identify if IPv6 is enabled on the system:

```
#!/usr/bin/env bash

{
    l_output=""
    ! grep -Pqs -- '^h*0\b' /sys/module/ipv6/parameters/disable &&
    l_output="- IPv6 is not enabled"
    if sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs --
    "^h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\b" && \
    sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs --
    "^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\b"; then
        l_output="- IPv6 is not enabled"
    fi
    [ -z "$l_output" ] && l_output="- IPv6 is enabled"
    echo -e "\n$l_output\n"
}
```

## Remediation:

Enable or disable IPv6 in accordance with system requirements and local site policy

## Default Value:

IPv6 is enabled

## References:

1. NIST SP 800-53 Rev. 5: CM-7

## Additional Information:

Having more addresses has grown in importance with the expansion of smart devices and connectivity. IPv6 provides more than enough globally unique IP addresses for every networked device currently on the planet, helping ensure providers can keep pace with the expected proliferation of IP-based devices.

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                   | Tactics | Mitigations |
|-----------------------------------------------|---------|-------------|
| T1557, T1557.000, T1595, T1595.001, T1595.002 | TA0008  | M1042       |



### *3.1.2 Ensure wireless interfaces are disabled (Automated)*

**Profile Applicability:**

- Level 1 - Server
- STIG

**Description:**

Wireless networking is used when wired networks are unavailable.

**Rationale:**

- **IF** - wireless is not to be used, wireless devices can be disabled to reduce the potential attack surface.

**Impact:**

Many if not all laptop workstations and some desktop workstations will connect via wireless requiring these interfaces be enabled.

**Audit:**

Run the following script to verify no wireless interfaces are active on the system:

```
#!/usr/bin/env bash

{
    l_output="" l_output2=""
    module_chk()
    {
        # Check how module will be loaded
        l_loadable="$(modprobe -n -v "$l_mname")"
        if grep -Pq -- '^h*install \/\bin\/(true|false)' <<< "$l_loadable";
then
            l_output="$l_output\n - module: \"$l_mname\" is not loadable:
\"$l_loadable\""
            else
                l_output2="$l_output2\n - module: \"$l_mname\" is loadable:
\"$l_loadable\""
            fi
            # Check is the module currently loaded
            if ! lsmod | grep "$l_mname" > /dev/null 2>&1; then
                l_output="$l_output\n - module: \"$l_mname\" is not loaded"
            else
                l_output2="$l_output2\n - module: \"$l_mname\" is loaded"
            fi
            # Check if the module is deny listed
            if modprobe --showconfig | grep -Pq -- "^h*blacklist\h+$l_mname\b";
then
                l_output="$l_output\n - module: \"$l_mname\" is deny listed in:
\"$(grep -Pl -- "^h*blacklist\h+$l_mname\b" /etc/modprobe.d/*)\"
            else
                l_output2="$l_output2\n - module: \"$l_mname\" is not deny listed"
            fi
        }
        if [ -n "$(find /sys/class/net/*/ -type d -name wireless)" ]; then
            l_dname=$(for driverdir in $(find /sys/class/net/*/ -type d -name
wireless | xargs -0 dirname); do basename "$(readlink -f
"$driverdir"/device/driver/module)";done | sort -u)
            for l_mname in $l_dname; do
                module_chk
            done
        fi
        # Report results. If no failures output in l_output2, we pass
        if [ -z "$l_output2" ]; then
            echo -e "\n- Audit Result:\n  ** PASS **"
            if [ -z "$l_output" ]; then
                echo -e "\n - System has no wireless NICs installed"
            else
                echo -e "\n$l_output\n"
            fi
        else
            echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
            [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
        fi
    }
}
```

## Remediation:

Run the following script to disable any wireless interfaces:

```
#!/usr/bin/env bash

{
    module_fix()
    {
        if ! modprobe -n -v "$l_mname" | grep -P -- '^\\h*install
\\bin\\/(true|false)'; then
            echo -e " - setting module: \"$l_mname\" to be un-loadable"
            echo -e "install $l_mname /bin/false" >>
/etc/modprobe.d/"$l_mname".conf
        fi
        if lsmod | grep "$l_mname" > /dev/null 2>&1; then
            echo -e " - unloading module \"$l_mname\""
            modprobe -r "$l_mname"
        fi
        if ! grep -Pq -- "\\h*blacklist\\h+$l_mname\\b" /etc/modprobe.d/*; then
            echo -e " - deny listing \"$l_mname\""
            echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mname".conf
        fi
    }
    if [ -n "$(find /sys/class/net/* -type d -name wireless)" ]; then
        l_dname=$(for driverdir in $(find /sys/class/net/* -type d -name
wireless | xargs -0 dirname); do basename "$(readlink -f
"$driverdir"/device/driver/module)";done | sort -u)
        for l_mname in $l_dname; do
            module_fix
        done
    fi
}
```

## References:

1. NIST SP 800-53 :: AC-18 (1)
2. NIST SP 800-53 :: AC-18 (1)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230506  
Rule ID: SV-230506r627750  
STIG ID: RHEL-08-040110  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                 | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.      |      | ●    | ●    |
| v7               | <b>15.4 <u>Disable Wireless Access on Devices if Not Required</u></b><br>Disable wireless access on devices that do not have a business purpose for wireless access.                                                                                                    |      |      | ●    |
| v7               | <b>15.5 <u>Limit Wireless Access on Client Devices</u></b><br>Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks. |      |      | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques                   | Tactics | Mitigations |
|-----------------------------------------------|---------|-------------|
| T1011, T1011.000, T1595, T1595.001, T1595.002 | TA0010  | M1028       |

### 3.1.3 Ensure bluetooth services are not in use (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 2 - Workstation

#### Description:

Bluetooth is a short-range wireless technology standard that is used for exchanging data between devices over short distances. It employs UHF radio waves in the ISM bands, from 2.402 GHz to 2.48 GHz. It is mainly used as an alternative to wire connections.

#### Rationale:

An attacker may be able to find a way to access or corrupt your data. One example of this type of activity is **bluesnarfing**, which refers to attackers using a Bluetooth connection to steal information off of your Bluetooth device. Also, viruses or other malicious code can take advantage of Bluetooth technology to infect other devices. If you are infected, your data may be corrupted, compromised, stolen, or lost.

#### Impact:

Many personal electronic devices (PEDs) use Bluetooth technology. For example, you may be able to operate your computer with a wireless keyboard. Disabling Bluetooth will prevent these devices from connecting to the system.

There may be packages that are dependent on the **bluez** package. If the **bluez** package is removed, these dependent packages will be removed as well. Before removing the **bluez** package, review any dependent packages to determine if they are required on the system.

- **IF** - a dependent package is required: stop and mask **bluetooth.service** leaving the **bluez** package installed.

## Audit:

Run the following command to verify the **bluez** package is not installed:

```
# rpm -q bluez  
  
package bluez is not installed
```

- OR -

- IF - the **bluez** package is required as a dependency:

Run the following command to verify **bluetooth.service** is not enabled:

```
# systemctl is-enabled bluetooth.service 2>/dev/null | grep 'enabled'  
  
Nothing should be returned
```

Run the following command to verify **bluetooth.service** is not active:

```
# systemctl is-active bluetooth.service 2>/dev/null | grep '^active'  
  
Nothing should be returned
```

**Note:** If the package is required for a dependency

- Ensure the dependent package is approved by local site policy
- Ensure stopping and masking the service and/or socket meets local site policy

## Remediation:

Run the following commands to stop **bluetooth.service**, and remove the **bluez** package:

```
# systemctl stop bluetooth.service  
# dnf remove bluez
```

- OR -

- IF - the **bluez** package is required as a dependency:

Run the following commands to stop and mask **bluetooth.service**:

```
# systemctl stop bluetooth.service  
# systemctl mask bluetooth.service
```

**Note:** A reboot may be required

## References:

1. NIST SP 800-53 Rev. 5: CM-7

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1011, T1011.001            | TA0010  | M1042       |

### 3.1.4 Ensure network interfaces are not in promiscuous mode (Manual)

**Profile Applicability:**

- STIG

**Description:**

Network interfaces must not be in promiscuous mode.

**Rationale:**

Network interfaces in promiscuous mode allow for the capture of all network traffic visible to the system. If unauthorized individuals can access these applications, it may allow them to collect information such as logon IDs, passwords, and key exchanges between systems.

If the system is being used to perform a network troubleshooting function, the use of these tools must be documented with the Information System Security Officer (ISSO) and restricted to only authorized personnel.

**Audit:**

Verify network interfaces are not in promiscuous mode unless approved by the ISSO and documented.

Check for the status with the following command:

```
# ip link | grep -i promisc
```

If network interfaces are found on the system in promiscuous mode and their use has not been approved by the ISSO and documented, this is a finding.

**Remediation:**

Configure network interfaces to turn off promiscuous mode unless approved by the ISSO and documented.

Set the promiscuous mode of an interface to off with the following command:

```
# ip link set dev <devicename> multicast off promisc off
```

**References:**

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)



Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230554  
Rule ID: SV-230554r627750  
STIG ID: RHEL-08-040330  
Severity: CAT II

CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | 4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | 9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## 3.2 Configure Network Kernel Modules

The Linux kernel modules support several network protocols that are not commonly used. If these protocols are not needed, it is recommended that they be disabled in the kernel.

**Note:** This should not be considered a comprehensive list of uncommon network protocols, you may wish to consider additions to those listed here for your environment.

### 3.2.1 Ensure dccp kernel module is not available (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

#### Description:

The Datagram Congestion Control Protocol (DCCP) is a transport layer protocol that supports streaming media and telephony. DCCP provides a way to gain access to congestion control, without having to do it at the application layer, but does not provide in-sequence delivery.

#### Rationale:

- **IF** - the protocol is not required, it is recommended that the drivers not be installed to reduce the potential attack surface.

#### Audit:

Run the following script to verify:

- **IF** - the **dccp** kernel module is available in ANY installed kernel, verify:

- An entry including **/bin/true** or **/bin/false** exists in a file within the **/etc/modprobe.d/** directory
- The module is deny listed in a file within the **/etc/modprobe.d/** directory
- The module is not loaded in the running kernel

- **IF** - the **dccp** kernel module is not available on the system, or pre-compiled into the kernel, no additional configuration is necessary

```

#!/usr/bin/env bash

{
    a_output=() a_output2=() a_output3=() l_dl="" l_mod_name="dccp"
    l_mod_type="net"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_chk()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if ! lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loaded")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loaded")
            fi
            if grep -Pq -- '\bbinstall\h+'${l_mod_chk_name//-/}_
/_}'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loadable")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loadable")
            fi
            if grep -Pq -- '\bbblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is deny listed")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is not deny listed")
            fi
        }
        for l_mod_base_directory in $l_mod_path; do
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name:-2"
                [ "$l_dl" != "y" ] && f_module_chk
            else
                a_output+=(" - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\"")
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        if [ "${#a_output2[@]}" -le 0 ]; then
            printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}"
        else
            printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
            [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "- Correctly set:"
"${a_output[@]}"
        fi
    }
}

```

## Remediation:

Run the following script to unload and disable the `dccp` module:

- **IF** - the `dccp` kernel module is available in ANY installed kernel:

- Create a file ending in `.conf` with `install dccp /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist dccp` in the `/etc/modprobe.d/` directory
- Run `modprobe -r dccp 2>/dev/null; rmmod dccp 2>/dev/null` to remove `dccp` from the kernel

- **IF** - the `dccp` kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

```
#!/usr/bin/env bash

{
  a_output2=() a_output3=() l_dl="" l_mod_name="dccc" l_mod_type="net"
  l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
  f_module_fix()
  {
    l_dl="y" a_showconfig=()
    while IFS= read -r l_showconfig; do
      a_showconfig+=("$l_showconfig")
      done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
      if lsmod | grep "$l_mod_chk_name" &> /dev/null; then
        a_output2+=(" - unloading kernel module: \"$l_mod_name\"")
        modprobe -r "$l_mod_chk_name" 2>/dev/null; rmmod "$l_mod_name"
2>/dev/null
      fi
      if ! grep -Pq -- '\binstall\h+'${l_mod_chk_name//-/}_
/_'\b'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
        a_output2+=(" - setting kernel module: \"$l_mod_name\" to
\"$(readlink -f /bin/false)\"")
        printf '%s\n' "install $l_mod_chk_name $(readlink -f /bin/false)" >>
/etc/modprobe.d/"$l_mod_name".conf
      fi
      if ! grep -Pq -- '\bblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
        a_output2+=(" - denylisting kernel module: \"$l_mod_name\"")
        printf '%s\n' "blacklist $l_mod_chk_name" >>
/etc/modprobe.d/"$l_mod_name".conf
      fi
    }
    for l_mod_base_directory in $l_mod_path; do # Check if the module exists
on the system
      if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
        a_output3+=(" - \"$l_mod_base_directory\"")
        l_mod_chk_name="$l_mod_name"
        [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="${l_mod_name::-2}"
        [ "$l_dl" != "y" ] && f_module_fix
      else
        printf '%s\n' " - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\""
      fi
    done
    [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
    [ "${#a_output2[@]}" -gt 0 ] && printf '%s\n' "" "${a_output2[@]}" ||
printf '%s\n' "" " - No changes needed"
    printf '%s\n' "" " - remediation of kernel module: \"$l_mod_name\"
complete" ""
  }
}
```

## References:

1. NIST SP 800-53 Rev. 5: SI-4, CM-7

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1068, T1068.000, T1210, T1210.000 | TA0008  | M1042       |

### 3.2.2 *Ensure tipc kernel module is not available (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

The Transparent Inter-Process Communication (TIPC) protocol is designed to provide communication between cluster nodes.

#### **Rationale:**

- **IF** - the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

#### **Audit:**

Run the following script to verify:

- **IF** - the **tipc** kernel module is available in ANY installed kernel, verify:

- An entry including **/bin/true** or **/bin/false** exists in a file within the **/etc/modprobe.d/** directory
- The module is deny listed in a file within the **/etc/modprobe.d/** directory
- The module is not loaded in the running kernel

- **IF** - the **tipc** kernel module is not available on the system, or pre-compiled into the kernel, no additional configuration is necessary



```

#!/usr/bin/env bash

{
    a_output=() a_output2=() a_output3=() l_dl="" l_mod_name="tipc"
    l_mod_type="net"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_chk()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_}''\b')
            if ! lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loaded")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loaded")
            fi
            if grep -Pq -- '\bbinstall\h+'${l_mod_chk_name//-/}_}''\b' <<<
"/_}"'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loadable")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loadable")
            fi
            if grep -Pq -- '\bbblacklist\h+'${l_mod_chk_name//-/}_}''\b' <<<
"${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is deny listed")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is not deny listed")
            fi
        }
        for l_mod_base_directory in $l_mod_path; do
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name:-2"
                [ "$l_dl" != "y" ] && f_module_chk
            else
                a_output+=(" - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\"")
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        if [ "${#a_output2[@]}" -le 0 ]; then
            printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}"
        else
            printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
            [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "- Correctly set:"
"${a_output[@]}"
        fi
    }
}

```

## Remediation:

Run the following script to unload and disable the `tipc` module:

- **IF** - the `tipc` kernel module is available in ANY installed kernel:

- Create a file ending in `.conf` with `install tipc /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist tipc` in the `/etc/modprobe.d/` directory
- Run `modprobe -r tipc 2>/dev/null; rmmod tipc 2>/dev/null` to remove `tipc` from the kernel

- **IF** - the `tipc` kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

```
#!/usr/bin/env bash

{
  a_output2=() a_output3=() l_dl="" l_mod_name="tipc" l_mod_type="net"
  l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
  f_module_fix()
  {
    l_dl="y" a_showconfig=()
    while IFS= read -r l_showconfig; do
      a_showconfig+=("$l_showconfig")
      done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
      if lsmod | grep "$l_mod_chk_name" &> /dev/null; then
        a_output2+=(" - unloading kernel module: \"$l_mod_name\"")
        modprobe -r "$l_mod_chk_name" 2>/dev/null; rmmod "$l_mod_name"
2>/dev/null
      fi
      if ! grep -Pq -- '\binstall\h+'${l_mod_chk_name//-/}_
/_'\b'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
        a_output2+=(" - setting kernel module: \"$l_mod_name\" to
\"$(readlink -f /bin/false)\"")
        printf '%s\n' "install $l_mod_chk_name $(readlink -f /bin/false)" >>
/etc/modprobe.d/"$l_mod_name".conf
      fi
      if ! grep -Pq -- '\bblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
        a_output2+=(" - denylisting kernel module: \"$l_mod_name\"")
        printf '%s\n' "blacklist $l_mod_chk_name" >>
/etc/modprobe.d/"$l_mod_name".conf
      fi
    }
    for l_mod_base_directory in $l_mod_path; do # Check if the module exists
on the system
      if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
        a_output3+=(" - \"$l_mod_base_directory\"")
        l_mod_chk_name="$l_mod_name"
        [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name::-2"
        [ "$l_dl" != "y" ] && f_module_fix
      else
        printf '%s\n' " - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\""
      fi
    done
    [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
    [ "${#a_output2[@]}" -gt 0 ] && printf '%s\n' "" "${a_output2[@]}" ||
printf '%s\n' "" " - No changes needed"
    printf '%s\n' "" " - remediation of kernel module: \"$l_mod_name\"
complete" ""
  }
}
```

## References:

1. NIST SP 800-53 :: CM-7
2. NIST SP 800-53A :: CM-7.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230497  
Rule ID: SV-230497r942927  
STIG ID: RHEL-08-040024  
Severity: CAT III

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1068, T1068.000, T1210, T1210.000 | TA0008  | M1042       |

### 3.2.3 Ensure rds kernel module is not available (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

#### Description:

The Reliable Datagram Sockets (RDS) protocol is a transport layer protocol designed to provide low-latency, high-bandwidth communications between cluster nodes. It was developed by the Oracle Corporation.

#### Rationale:

- **IF** - the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

#### Audit:

Run the following script to verify:

- **IF** - the **rds** kernel module is available in ANY installed kernel, verify:

- An entry including **/bin/true** or **/bin/false** exists in a file within the **/etc/modprobe.d/** directory
- The module is deny listed in a file within the **/etc/modprobe.d/** directory
- The module is not loaded in the running kernel

- **IF** - the **rds** kernel module is not available on the system, or pre-compiled into the kernel, no additional configuration is necessary

```

#!/usr/bin/env bash

{
    a_output=() a_output2=() a_output3=() l_dl="" l_mod_name="rds"
    l_mod_type="net"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_chk()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if ! lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loaded")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loaded")
            fi
            if grep -Pq -- '\bbinstall\h+'${l_mod_chk_name//-/}_
/_}'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loadable")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loadable")
            fi
            if grep -Pq -- '\bbblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is deny listed")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is not deny listed")
            fi
        }
        for l_mod_base_directory in $l_mod_path; do
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name:-2"
                [ "$l_dl" != "y" ] && f_module_chk
            else
                a_output+=(" - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\"")
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        if [ "${#a_output2[@]}" -le 0 ]; then
            printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}"
        else
            printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
            [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "- Correctly set:"
"${a_output[@]}"
        fi
    }
}

```

## Remediation:

Run the following script to unload and disable the `rds` module:

- **IF** - the `rds` kernel module is available in ANY installed kernel:

- Create a file ending in `.conf` with `install rds /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist rds` in the `/etc/modprobe.d/` directory
- Run `modprobe -r rds 2>/dev/null; rmmod rds 2>/dev/null` to remove `rds` from the kernel

- **IF** - the `rds` kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

```
#!/usr/bin/env bash

{
  a_output2=() a_output3=() l_dl="" l_mod_name="rds" l_mod_type="net"
  l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
  f_module_fix()
  {
    l_dl="y" a_showconfig=()
    while IFS= read -r l_showconfig; do
      a_showconfig+=("$l_showconfig")
      done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
      if lsmod | grep "$l_mod_chk_name" &> /dev/null; then
        a_output2+=(" - unloading kernel module: \"$l_mod_name\"")
        modprobe -r "$l_mod_chk_name" 2>/dev/null; rmmod "$l_mod_name"
2>/dev/null
      fi
      if ! grep -Pq -- '\binstall\h+'${l_mod_chk_name//-/}_
/_'\b'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
        a_output2+=(" - setting kernel module: \"$l_mod_name\" to
\"$(readlink -f /bin/false)\"")
        printf '%s\n' "install $l_mod_chk_name $(readlink -f /bin/false)" >>
/etc/modprobe.d/"$l_mod_name".conf
      fi
      if ! grep -Pq -- '\bblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
        a_output2+=(" - denylisting kernel module: \"$l_mod_name\"")
        printf '%s\n' "blacklist $l_mod_chk_name" >>
/etc/modprobe.d/"$l_mod_name".conf
      fi
    }
    for l_mod_base_directory in $l_mod_path; do # Check if the module exists
on the system
      if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
        a_output3+=(" - \"$l_mod_base_directory\"")
        l_mod_chk_name="$l_mod_name"
        [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="${l_mod_name::-2}"
        [ "$l_dl" != "y" ] && f_module_fix
      else
        printf '%s\n' " - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\""
      fi
    done
    [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
    [ "${#a_output2[@]}" -gt 0 ] && printf '%s\n' "" "${a_output2[@]}" ||
printf '%s\n' "" " - No changes needed"
    printf '%s\n' "" " - remediation of kernel module: \"$l_mod_name\"
complete" ""
  }
}
```

## References:

1. NIST SP 800-53 Rev. 5: SI-4, CM-7



**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1068, T1068.000, T1210, T1210.000 | TA0008  | M1042       |

### 3.2.4 Ensure sctp kernel module is not available (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### Description:

The Stream Control Transmission Protocol (SCTP) is a transport layer protocol used to support message oriented communication, with several streams of messages in one connection. It serves a similar function as TCP and UDP, incorporating features of both. It is message-oriented like UDP, and ensures reliable in-sequence transport of messages with congestion control like TCP.

#### Rationale:

- **IF** - the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

#### Audit:

Run the following script to verify:

- **IF** - the **sctp** kernel module is available in ANY installed kernel, verify:

- An entry including **/bin/true** or **/bin/false** exists in a file within the **/etc/modprobe.d/** directory
- The module is deny listed in a file within the **/etc/modprobe.d/** directory
- The module is not loaded in the running kernel

- **IF** - the **sctp** kernel module is not available on the system, or pre-compiled into the kernel, no additional configuration is necessary

```

#!/usr/bin/env bash

{
    a_output=() a_output2=() a_output3=() l_dl="" l_mod_name="sctp"
    l_mod_type="net"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_chk()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if ! lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loaded")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loaded")
            fi
            if grep -Pq -- '\bbinstall\h+'${l_mod_chk_name//-/}_
/_}'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loadable")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loadable")
            fi
            if grep -Pq -- '\bbblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is deny listed")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is not deny listed")
            fi
        }
        for l_mod_base_directory in $l_mod_path; do
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name:-2"
                [ "$l_dl" != "y" ] && f_module_chk
            else
                a_output+=(" - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\"")
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        if [ "${#a_output2[@]}" -le 0 ]; then
            printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}"
        else
            printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
            [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "- Correctly set:"
"${a_output[@]}"
        fi
    }
}

```

## Remediation:

Run the following script to unload and disable the `sctp` module:

- **IF** - the `sctp` kernel module is available in ANY installed kernel:

- Create a file ending in `.conf` with `install sctp /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist sctp` in the `/etc/modprobe.d/` directory
- Run `modprobe -r sctp 2>/dev/null; rmmod sctp 2>/dev/null` to remove `sctp` from the kernel

- **IF** - the `sctp` kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

```
#!/usr/bin/env bash

{
  a_output2=() a_output3=() l_dl="" l_mod_name="sctp" l_mod_type="net"
  l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
  f_module_fix()
  {
    l_dl="y" a_showconfig=()
    while IFS= read -r l_showconfig; do
      a_showconfig+=("$l_showconfig")
      done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
      if lsmod | grep "$l_mod_chk_name" &> /dev/null; then
        a_output2+=(" - unloading kernel module: \"$l_mod_name\"")
        modprobe -r "$l_mod_chk_name" 2>/dev/null; rmmod "$l_mod_name"
2>/dev/null
      fi
      if ! grep -Pq -- '\binstall\h+'${l_mod_chk_name//-/}_
/_'\b'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
        a_output2+=(" - setting kernel module: \"$l_mod_name\" to
\"$(readlink -f /bin/false)\"")
        printf '%s\n' "install $l_mod_chk_name $(readlink -f /bin/false)" >>
/etc/modprobe.d/"$l_mod_name".conf
      fi
      if ! grep -Pq -- '\bblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
        a_output2+=(" - denylisting kernel module: \"$l_mod_name\"")
        printf '%s\n' "blacklist $l_mod_chk_name" >>
/etc/modprobe.d/"$l_mod_name".conf
      fi
    }
    for l_mod_base_directory in $l_mod_path; do # Check if the module exists
on the system
      if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
        a_output3+=(" - \"$l_mod_base_directory\"")
        l_mod_chk_name="$l_mod_name"
        [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name::-2"
        [ "$l_dl" != "y" ] && f_module_fix
      else
        printf '%s\n' " - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\""
      fi
    done
    [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
    [ "${#a_output2[@]}" -gt 0 ] && printf '%s\n' "" "${a_output2[@]}" ||
printf '%s\n' "" " - No changes needed"
    printf '%s\n' "" " - remediation of kernel module: \"$l_mod_name\"
complete" ""
  }
}
```

## References:

1. NIST SP 800-53 :: CM-7
2. NIST SP 800-53A :: CM-7.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230496  
Rule ID: SV-230496r942924  
STIG ID: RHEL-08-040023  
Severity: CAT III

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1068, T1068.000, T1210, T1210.000 | TA0008  | M1042       |

### 3.2.5 Ensure atm kernel module is not available (Automated)

#### Profile Applicability:

- STIG

#### Description:

The Asynchronous Transfer Mode (ATM) is a protocol operating on network, data link, and physical layers, based on virtual circuits and virtual paths. Disabling ATM protects the system against exploitation of any flaws in its implementation.

#### Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Failing to disconnect unused protocols can result in a system compromise.

#### Audit:

Run the following script to verify:

- **IF** - the **atm** kernel module is available in ANY installed kernel, verify:

- An entry including **/bin/true** or **/bin/false** exists in a file within the **/etc/modprobe.d/** directory
- The module is deny listed in a file within the **/etc/modprobe.d/** directory
- The module is not loaded in the running kernel

- **IF** - the **atm** kernel module is not available on the system, or pre-compiled into the kernel, no additional configuration is necessary

```

#!/usr/bin/env bash

{
    a_output=() a_output2=() a_output3=() l_dl="" l_mod_name="atm"
    l_mod_type="net"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_chk()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if ! lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loaded")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loaded")
            fi
            if grep -Pq -- '\bbinstall\h+'${l_mod_chk_name//-/}_
/_}'\h+(\usr)?\bin\(/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loadable")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loadable")
            fi
            if grep -Pq -- '\bbblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is deny listed")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is not deny listed")
            fi
        }
        for l_mod_base_directory in $l_mod_path; do
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name:-2"
                [ "$l_dl" != "y" ] && f_module_chk
            else
                a_output+=(" - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\"")
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        if [ "${#a_output2[@]}" -le 0 ]; then
            printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}"
        else
            printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
            [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "- Correctly set:"
"${a_output[@]}"
        fi
    }
}

```



## Remediation:

Run the following script to unload and disable the `atm` module:

- **IF** - the `atm` kernel module is available in ANY installed kernel:

- Create a file ending in `.conf` with `install atm /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist atm` in the `/etc/modprobe.d/` directory
- Run `modprobe -r atm 2>/dev/null; rmmod atm 2>/dev/null` to remove `atm` from the kernel

- **IF** - the `atm` kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

```
#!/usr/bin/env bash

{
    a_output2=() a_output3=() l_dl="" l_mod_name="atm" l_mod_type="net"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_fix()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output2+=(" - unloading kernel module: \"$l_mod_name\"")
                modprobe -r "$l_mod_chk_name" 2>/dev/null; rmmod "$l_mod_name"
2>/dev/null
            fi
            if ! grep -Pq -- '\binstall\h+'${l_mod_chk_name//-/}_
/_'\b'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output2+=(" - setting kernel module: \"$l_mod_name\" to
\"$(readlink -f /bin/false)\"")
                printf '%s\n' "install $l_mod_chk_name $(readlink -f /bin/false)" >>
/etc/modprobe.d/"$l_mod_name".conf
            fi
            if ! grep -Pq -- '\bblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output2+=(" - denylisting kernel module: \"$l_mod_name\"")
                printf '%s\n' "blacklist $l_mod_chk_name" >>
/etc/modprobe.d/"$l_mod_name".conf
            fi
        }
        for l_mod_base_directory in $l_mod_path; do # Check if the module exists
on the system
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name::-2"
                [ "$l_dl" != "y" ] && f_module_fix
            else
                printf '%s\n' " - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\""
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        [ "${#a_output2[@]}" -gt 0 ] && printf '%s\n' "" "${a_output2[@]}" ||
printf '%s\n' "" " - No changes needed"
        printf '%s\n' "" " - remediation of kernel module: \"$l_mod_name\"
complete" ""
    }
}
```

Reboot the system for the settings to take effect.

## References:

1. NIST SP 800-53 Revision 5 :: CM-7 a
2. NIST SP 800-53A :: CM-7.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230494  
Rule ID: SV-230494r942918  
STIG ID: RHEL-08-040021  
Severity: CAT III

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |    |    |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

### *3.2.6 Ensure bluetooth kernel module is not available (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Bluetooth is a short-range wireless technology standard that is used for exchanging data between devices over short distances. It employs UHF radio waves in the ISM bands, from 2.402 GHz to 2.48 GHz. It is mainly used as an alternative to wire connections.

#### **Rationale:**

Without protection of communications with wireless peripherals, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read, altered, or used to compromise the operating system.

This requirement applies to wireless peripheral technologies (e.g., wireless mice, keyboards, displays, etc.) used with RHEL 8 operating systems. Wireless peripherals (e.g., Wi-Fi/Bluetooth/IR Keyboards, Mice, and Pointing Devices and Near Field Communications [NFC]) present a unique challenge by creating an open, unsecured port on a computer. Wireless peripherals must meet DoD requirements for wireless data transmission and be approved for use by the Authorizing Official (AO). Even though some wireless peripherals, such as mice and pointing devices, do not ordinarily carry information that need to be protected, modification of communications with these wireless peripherals may be used to compromise the operating system. Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of communications with wireless peripherals can be accomplished by physical means (e.g., employing physical barriers to wireless radio frequencies) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa. If the wireless peripheral is only passing telemetry data, encryption of the data may not be required.

#### **Impact:**

Many personal electronic devices (PEDs) use Bluetooth technology. For example, you may be able to operate your computer with a wireless keyboard. Disabling Bluetooth will prevent these devices from connecting to the system.

## Audit:

If the device or operating system does not have a Bluetooth adapter installed, this requirement is not applicable.

This requirement is not applicable to mobile devices (smartphones and tablets), where the use of Bluetooth is a local AO decision.

Determine if Bluetooth is disabled with the following command:

```
# grep bluetooth /etc/modprobe.d/*  
  
/etc/modprobe.d/bluetooth.conf:install bluetooth /bin/true
```

If the Bluetooth driver blacklist entry is missing, a Bluetooth driver is determined to be in use, and the collaborative computing device has not been authorized for use, this is a finding.

Run the following script to verify:

- **IF** - the **tipc** kernel module is available in ANY installed kernel, verify:

- An entry including **/bin/true** or **/bin/false** exists in a file within the **/etc/modprobe.d/** directory
- The module is deny listed in a file within the **/etc/modprobe.d/** directory
- The module is not loaded in the running kernel

- **IF** - the **tipc** kernel module is not available on the system, or pre-compiled into the kernel, no additional configuration is necessary

```

#!/usr/bin/env bash

{
    a_output=() a_output2=() a_output3=() l_dl="" l_mod_name="tipc"
    l_mod_type="net"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_chk()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if ! lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loaded")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loaded")
            fi
            if grep -Pq -- '\bbinstall\h+'${l_mod_chk_name//-/}_
/_}'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loadable")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loadable")
            fi
            if grep -Pq -- '\bbblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is deny listed")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is not deny listed")
            fi
        }
        for l_mod_base_directory in $l_mod_path; do
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name:-2"
                [ "$l_dl" != "y" ] && f_module_chk
            else
                a_output+=(" - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\"")
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        if [ "${#a_output2[@]}" -le 0 ]; then
            printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}"
        else
            printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
            [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "- Correctly set:"
"${a_output[@]}"
        fi
    }
}

```

## Remediation:

Configure the operating system to disable the Bluetooth adapter when not in use. Build or modify the "/etc/modprobe.d/bluetooth.conf" file with the following line:

```
install bluetooth /bin/true
```

Run the following script to unload and disable the **bluetooth** module:

- **IF** - the **bluetooth** kernel module is available in ANY installed kernel:

- Create a file ending in **.conf** with **install bluetooth /bin/false** in the **/etc/modprobe.d/** directory
- Create a file ending in **.conf** with **blacklist bluetooth** in the **/etc/modprobe.d/** directory
- Run **modprobe -r bluetooth 2>/dev/null; rmmod bluetooth 2>/dev/null** to remove **bluetooth** from the kernel

- **IF** - the **bluetooth** kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

```
#!/usr/bin/env bash

{
    a_output2=() a_output3=() l_dl="" l_mod_name="bluetooth" l_mod_type="net"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_fix()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output2+=(" - unloading kernel module: \"$l_mod_name\"")
                modprobe -r "$l_mod_chk_name" 2>/dev/null; rmmod "$l_mod_name"
2>/dev/null
            fi
            if ! grep -Pq -- '\binstall\h+'${l_mod_chk_name//-/}_
/_}'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output2+=(" - setting kernel module: \"$l_mod_name\" to
\"$(readlink -f /bin/false)\"")
                printf '%s\n' "install $l_mod_chk_name $(readlink -f /bin/false)" >>
/etc/modprobe.d/"$l_mod_name".conf
            fi
            if ! grep -Pq -- '\bblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output2+=(" - denylisting kernel module: \"$l_mod_name\"")
                printf '%s\n' "blacklist $l_mod_chk_name" >>
/etc/modprobe.d/"$l_mod_name".conf
            fi
        }
        for l_mod_base_directory in $l_mod_path; do # Check if the module exists
on the system
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="${l_mod_name::-2}"
                [ "$l_dl" != "y" ] && f_module_fix
            else
                printf '%s\n' " - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\""
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        [ "${#a_output2[@]}" -gt 0 ] && printf '%s\n' "" "${a_output2[@]}" ||
printf '%s\n' "" " - No changes needed"
        printf '%s\n' "" " - remediation of kernel module: \"$l_mod_name\"
complete" ""
    }
}
```

Reboot the system for the settings to take effect.



## References:

1. NIST SP 800-53 Revision 5 :: AC-18 (1)
2. NIST SP 800-53A :: AC-18 (1).1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230507  
Rule ID: SV-230507r942939  
STIG ID: RHEL-08-040111  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |    |    |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

### 3.2.7 Ensure can kernel module is not available (Automated)

#### Profile Applicability:

- STIG

#### Description:

The Controller Area Network (CAN) is a serial communications protocol, which was initially developed for automotive and is now also used in marine, industrial, and medical applications. Disabling CAN protects the system against exploitation of any flaws in its implementation.

#### Rationale:

It is detrimental for operating systems to provide, or install by default, functionality exceeding requirements or mission objectives. These unnecessary capabilities or services are often overlooked and therefore may remain unsecured. They increase the risk to the platform by providing additional attack vectors.

Failing to disconnect unused protocols can result in a system compromise.

#### Audit:

Run the following script to verify:

- **IF** - the **can** kernel module is available in ANY installed kernel, verify:

- An entry including **/bin/true** or **/bin/false** exists in a file within the **/etc/modprobe.d/** directory
- The module is deny listed in a file within the **/etc/modprobe.d/** directory
- The module is not loaded in the running kernel

- **IF** - the **can** kernel module is not available on the system, or pre-compiled into the kernel, no additional configuration is necessary

```

#!/usr/bin/env bash

{
    a_output=() a_output2=() a_output3=() l_dl="" l_mod_name="can"
    l_mod_type="net"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_chk()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if ! lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loaded")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loaded")
            fi
            if grep -Pq -- '\bbinstall\h+'${l_mod_chk_name//-/}_
/_}'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is not loadable")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is loadable")
            fi
            if grep -Pq -- '\bbblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output+=(" - kernel module: \"$l_mod_name\" is deny listed")
            else
                a_output2+=(" - kernel module: \"$l_mod_name\" is not deny listed")
            fi
        }
        for l_mod_base_directory in $l_mod_path; do
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="$l_mod_name:-2"
                [ "$l_dl" != "y" ] && f_module_chk
            else
                a_output+=(" - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\"")
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        if [ "${#a_output2[@]}" -le 0 ]; then
            printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}"
        else
            printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
            [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "- Correctly set:"
"${a_output[@]}"
        fi
    }
}

```

## Remediation:

Configure the operating system to disable the ability to use the CAN protocol kernel module.

Add or update the following lines in the file `"/etc/modprobe.d/blacklist.conf"`:

```
install can /bin/false
blacklist can
```

Run the following script to unload and disable the `can` module:

- **IF** - the `can` kernel module is available in ANY installed kernel:

- Create a file ending in `.conf` with `install can /bin/false` in the `/etc/modprobe.d/` directory
- Create a file ending in `.conf` with `blacklist can` in the `/etc/modprobe.d/` directory
- Run `modprobe -r can 2>/dev/null; rmmod can 2>/dev/null` to remove `can` from the kernel

- **IF** - the `can` kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

```
#!/usr/bin/env bash

{
    a_output2=() a_output3=() l_dl="" l_mod_name="can" l_mod_type="net"
    l_mod_path="$(readlink -f /lib/modules/**/kernel/$l_mod_type | sort -u)"
    f_module_fix()
    {
        l_dl="y" a_showconfig=()
        while IFS= read -r l_showconfig; do
            a_showconfig+=("$l_showconfig")
            done < <(modprobe --showconfig | grep -P --
'\b(install|blacklist)\h+'${l_mod_chk_name//-/}_'\b')
            if lsmod | grep "$l_mod_chk_name" &> /dev/null; then
                a_output2+=(" - unloading kernel module: \"$l_mod_name\"")
                modprobe -r "$l_mod_chk_name" 2>/dev/null; rmmod "$l_mod_name"
2>/dev/null
            fi
            if ! grep -Pq -- '\binstall\h+'${l_mod_chk_name//-/}_
/_'\b'\h+(\usr)?\bin\/(true|false)\b' <<< "${a_showconfig[*]}"; then
                a_output2+=(" - setting kernel module: \"$l_mod_name\" to
\"$(readlink -f /bin/false)\"")
                printf '%s\n' "install $l_mod_chk_name $(readlink -f /bin/false)" >>
/etc/modprobe.d/"$l_mod_name".conf
            fi
            if ! grep -Pq -- '\bblacklist\h+'${l_mod_chk_name//-/}_'\b' <<<
"${a_showconfig[*]}"; then
                a_output2+=(" - denylisting kernel module: \"$l_mod_name\"")
                printf '%s\n' "blacklist $l_mod_chk_name" >>
/etc/modprobe.d/"$l_mod_name".conf
            fi
        }
        for l_mod_base_directory in $l_mod_path; do # Check if the module exists
on the system
            if [ -d "$l_mod_base_directory/${l_mod_name//-/}/" ] && [ -n "$(ls -A
"$l_mod_base_directory/${l_mod_name//-/}/")" ]; then
                a_output3+=(" - \"$l_mod_base_directory\"")
                l_mod_chk_name="$l_mod_name"
                [[ "$l_mod_name" =~ overlay ]] && l_mod_chk_name="${l_mod_name::-2}"
                [ "$l_dl" != "y" ] && f_module_fix
            else
                printf '%s\n' " - kernel module: \"$l_mod_name\" doesn't exist in
\"$l_mod_base_directory\""
            fi
        done
        [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" " -- INFO --" " - module:
\"$l_mod_name\" exists in:" "${a_output3[@]}"
        [ "${#a_output2[@]}" -gt 0 ] && printf '%s\n' "" "${a_output2[@]}" ||
printf '%s\n' "" " - No changes needed"
        printf '%s\n' "" " - remediation of kernel module: \"$l_mod_name\"
complete" ""
    }
}
```

Reboot the system for the settings to take effect.

## References:

1. NIST SP 800-53 :: CM-7
2. NIST SP 800-53A :: CM-7.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230495  
Rule ID: SV-230495r942921  
STIG ID: RHEL-08-040022  
Severity: CAT III

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |    |    |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

### 3.3 Configure Network Kernel Parameters

The following network parameters are intended for use on both host only and router systems. A system acts as a router if it has at least two interfaces and is configured to perform routing functions.

#### Notes:

- sysctl settings are defined through files in `/usr/local/lib`, `/usr/lib`, `/lib`, `/run`, and `/etc`
- Files are typically placed in the `sysctl.d` directory within the parent directory
- The paths where sysctl preload files usually exist
  - `/run/sysctl.d/*.conf`
  - `/etc/sysctl.d/*.conf`
  - `/usr/local/lib/sysctl.d/*.conf`
  - `/usr/lib/sysctl.d/*.conf`
  - `/lib/sysctl.d/*.conf`
  - `/etc/sysctl.conf`
- Files must have the `".conf"` extension
- Vendors settings usually live in `/usr/lib` or `/usr/local/lib`
- To override a whole file, create a new file with the same name in `/etc/sysctl.d/` and put new settings there.
- To override only specific settings, add a file with a lexically later name in `/etc/sysctl.d/` and put new settings there.
- The command `/usr/lib/systemd/systemd-sysctl --cat-config` produces output containing The system's loaded kernel parameters and the files they're configured in:
  - Entries listed latter in the file take precedence over the same settings listed earlier in the file
  - Files containing kernel parameters that are over-ridden by other files with the same name will not be listed
  - On systems running UncomplicatedFirewall, the kernel parameters may be set or over-written. This will not be visible in the output of the command
- On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`
  - The settings in `/etc/ufw/sysctl.conf` will override settings other settings and **will not** be visible in the output of the `/usr/lib/systemd/systemd-sysctl --cat-config` command
  - This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

The system's loaded kernel parameters and the files they're configured in can be viewed by running the following command:

```
# /usr/lib/systemd/systemd-sysctl --cat-config
```

### 3.3.1 Ensure ip forwarding is disabled (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The `net.ipv4.ip_forward` and `net.ipv6.conf.all.forwarding` flags are used to tell the system whether it can forward packets or not.

#### Rationale:

Setting `net.ipv4.ip_forward` and `net.ipv6.conf.all.forwarding` to `0` ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

#### Impact:

IP forwarding is required on systems configured to act as a router. If these parameters are disabled, the system will not be able to perform as a router.

Many Cloud Service Provider (CSP) hosted systems require IP forwarding to be enabled. If the system is running on a CSP platform, this requirement should be reviewed before disabling IP forwarding.

#### Audit:

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.ip_forward` is set to `0`
- `net.ipv6.conf.all.forwarding` is set to `0`

#### Note:

- kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.
- IPv6 kernel parameters only apply to systems where IPv6 is enabled



```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); l_ipv6_disabled=""
    a_parlist=("net.ipv4.ip_forward=0" "net.ipv6.conf.all.forwarding=0")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    f_ipv6_chk()
    {
        l_ipv6_disabled="no"
        ! grep -Pqs -- '^\h*0\b' /sys/module/ipv6/parameters/disable &&
l_ipv6_disabled="yes"
        if sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs --
"^\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\b" && \
            sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs --
"^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\b"; then
            l_ipv6_disabled="yes"
        fi
    }
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F=
'{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\"")
            "    in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"") \
            "    in the running configuration" \
            "    and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="$l_out//# /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=(["$l_kpar"]="$l_file")
                fi
            fi
            done < <("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([\^#\n\r]+|[\^#\n\r\/[\^#\n\r\h]+\.\conf\b)')
            if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
                l_kpar="$(grep -Po "^\h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
                l_kpar="$l_kpar//\./}"
                [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=(["$l_kpar"]="$l_ufwscf")
            fi
            if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
                while IFS="=" read -r l_fkpname l_file_parameter_value; do

```

```

        l_fkpname="${l_fkpname// /}";
l_file_parameter_value="${l_file_parameter_value// /}"
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_file_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\" \" \" \
                " in \"$(printf '%s' "${A_out[@]})\" \" \"")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\" \" \" \
                " in \"$(printf '%s' "${A_out[@]})\" \" \" \" \
                " and should have a value of: \"$l_value_out\" \" \"")
        fi
        done < <(grep -Po -- "^\\h*$l_parameter_name\\h*=\\h*\\H+"
"${A_out[@]})"
        else
            a_output2+=(" - \"$l_parameter_name\" is not set in an included
file\" \" \
                " ** Note: \"$l_parameter_name\" May be set in a file that's
ignored by load procedure **")
        fi
    }
    l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
    while IFS="" read -r l_parameter_name l_parameter_value; do # Assess and
check parameters
        l_parameter_name="${l_parameter_name// /}";
l_parameter_value="${l_parameter_value// /}"
        l_value_out="${l_parameter_value//-/ through }";
l_value_out="${l_value_out//|/ or }"
        l_value_out="$(tr -d '(){}' <<< "$l_value_out")"
        if grep -q '^net.ipv6.' <<< "$l_parameter_name"; then
            [ -z "$l_ipv6_disabled" ] && f_ipv6_chk
            if [ "$l_ipv6_disabled" = "yes" ]; then
                a_output+=(" - IPv6 is disabled on the system,
\"$l_parameter_name\" is not applicable")
            else
                f_kernel_parameter_chk
            fi
        else
            f_kernel_parameter_chk
        fi
        done < <(printf '%s\\n' "${a_parlist[@]})"
        if [ "${#a_output2[@]}" -le 0 ]; then
            printf '%s\\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
        else
            printf '%s\\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
            [ "${#a_output2[@]}" -gt 0 ] && printf '%s\\n' "" "- Correctly set:"
"${a_output[@]}" ""
        fi
    }
}

```

## Remediation:

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv4.ip_forward = 0`

### Example:

```
# printf '%s\n' "net.ipv4.ip_forward = 0" >> /etc/sysctl.d/60-netip4_sysctl.conf
```

Run the following script to set the active kernel parameters:

```
#!/usr/bin/env bash

{
    sysctl -w net.ipv4.ip_forward=0
    sysctl -w net.ipv4.route.flush=1
}
```

- IF - IPv6 is enabled on the system:

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv6.conf.all.forwarding = 0`

### Example:

```
# printf '%s\n' "net.ipv6.conf.all.forwarding = 0" >> /etc/sysctl.d/60-netip6_sysctl.conf
```

Run the following script to set the active kernel parameters:

```
#!/usr/bin/env bash

{
    sysctl -w net.ipv6.conf.all.forwarding=0
    sysctl -w net.ipv6.route.flush=1
}
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## Default Value:

`net.ipv4.ip_forward = 0`

`net.ipv6.conf.all.forwarding = 0`

## References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230540  
Rule ID: SV-230540r858810  
STIG ID: RHEL-08-040260  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      | ●    | ●    |
| v7               | <u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics        | Mitigations  |
|-----------------------------|----------------|--------------|
| T1557, T1557.000            | TA0006, TA0009 | M1030, M1042 |

### 3.3.2 *Ensure packet redirect sending is disabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### **Description:**

ICMP Redirects are used to send routing information to other hosts. As a host itself does not act as a router (in a host only configuration), there is no need to send redirects.

#### **Rationale:**

An attacker could use a compromised host to send invalid ICMP redirects to other router devices in an attempt to corrupt routing and have users access a system set up by the attacker as opposed to a valid system.

#### **Impact:**

IP forwarding is required on systems configured to act as a router. If these parameters are disabled, the system will not be able to perform as a router.

#### **Audit:**

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.conf.all.send_redirects` is set to `0`
- `net.ipv4.conf.default.send_redirects` is set to `0`

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); l_ipv6_disabled=""
    a_parlist=("net.ipv4.conf.all.send_redirects=0"
"net.ipv4.conf.default.send_redirects=0")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print
$2}' /etc/default/ufw)"
    f_ipv6_chk()
    {
        l_ipv6_disabled="no"
        ! grep -Pqs -- '^h*0\b' /sys/module/ipv6/parameters/disable &&
l_ipv6_disabled="yes"
        if sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs --
"^h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\b" && \
            sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs --
"^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\b"; then
            l_ipv6_disabled="yes"
        fi
    }
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F=
'{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\""
                " in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"" \
                " in the running configuration" \
                " and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//# /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ] = "$l_file")
                fi
            fi
            done < <("$l_systemdsysctl" --cat-config | grep -Po
'^h*([\#\n\r]+|[\#\h*\[/^\#\n\r\h]+\.\conf\b)')
            if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
                l_kpar="$(grep -Po '^h*$l_parameter_name\b' "$l_ufwscf" | xargs)"
                l_kpar="${l_kpar//\\/\\.}"
                [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ] = "$l_ufwscf")
            fi
            if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output

```



## Remediation:

Set the following parameters in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv4.conf.all.send_redirects = 0`
- `net.ipv4.conf.default.send_redirects = 0`

### Example:

```
# printf '%s\n' "net.ipv4.conf.all.send_redirects = 0"
"net.ipv4.conf.default.send_redirects = 0" >> /etc/sysctl.d/60-
netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

```
#!/usr/bin/env bash

{
    sysctl -w net.ipv4.conf.all.send_redirects=0
    sysctl -w net.ipv4.conf.default.send_redirects=0
    sysctl -w net.ipv4.route.flush=1
}
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## Default Value:

`net.ipv4.conf.all.send_redirects = 1`

`net.ipv4.conf.default.send_redirects = 1`

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)



## Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

GROUP ID: V-230536  
RULE ID: SV-230536r858795  
STIG ID: RHEL-08-040220  
SEVERITY: CAT II

GROUP ID: V-230543  
RULE ID: SV-230543r858816  
STIG ID: RHEL-08-040270  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      | ●    | ●    |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics        | Mitigations  |
|-----------------------------|----------------|--------------|
| T1557, T1557.000            | TA0006, TA0009 | M1030, M1042 |

### 3.3.3 *Ensure bogus icmp responses are ignored (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Setting `net.ipv4.icmp_ignore_bogus_error_responses` to `1` prevents the kernel from logging bogus responses (RFC-1122 non-compliant) from broadcast reframes, keeping file systems from filling up with useless log messages.

#### **Rationale:**

Some routers (and some attackers) will send responses that violate RFC-1122 and attempt to fill up a log file system with many useless error messages.

#### **Audit:**

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.icmp_ignore_bogus_error_responses` is set to `1`

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); l_ipv6_disabled=""
    a_parlist=("net.ipv4.icmp_ignore_bogus_error_responses=1")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    f_ipv6_chk()
    {
        l_ipv6_disabled="no"
        ! grep -Pqs -- '^h*0\b' /sys/module/ipv6/parameters/disable &&
l_ipv6_disabled="yes"
        if sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs --
'^h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\b' && \
            sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs --
'^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\b'; then
            l_ipv6_disabled="yes"
        fi
    }
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F=
'{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\"")
            "    in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"") \
            "    in the running configuration" \
            "    and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="$l_out//# /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=(["$l_kpar"]="$l_file")
                fi
            fi
            done < <("$l_systemdsysctl" --cat-config | grep -Po
'^h*([\^#\n\r]+|#[h*\n\r\h]+\n.conf\b)')
            if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
                l_kpar="$(grep -Po '^h*$l_parameter_name\b' "$l_ufwscf" | xargs)"
                l_kpar="$l_kpar//.}"
                [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=(["$l_kpar"]="$l_ufwscf")
            fi
            if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
                while IFS="=" read -r l_fkpname l_file_parameter_value; do

```

```

        l_fkpname="${l_fkpname// /}";
l_file_parameter_value="${l_file_parameter_value// /}"
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_file_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\" \" \" \"
                in \"$(printf '%s' "${A_out[@]})\" \" \")
            else
                a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\" \" \"
                in \"$(printf '%s' "${A_out[@]})\" \" \" \"
                and should have a value of: \"$l_value_out\" \" \")
            fi
        done < <(grep -Po -- "^\\h*$l_parameter_name\\h*=\\h*\\H+"
"${A_out[@]})"
        else
            a_output2+=(" - \"$l_parameter_name\" is not set in an included
file\" \"
                \" ** Note: \"$l_parameter_name\" May be set in a file that's
ignored by load procedure **\")
        fi
    }
    l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
    while IFS="" read -r l_parameter_name l_parameter_value; do # Assess and
check parameters
        l_parameter_name="${l_parameter_name// /}";
l_parameter_value="${l_parameter_value// /}"
        l_value_out="${l_parameter_value//-/ through }";
l_value_out="${l_value_out//|/ or }"
        l_value_out="$(tr -d '(){}' <<< "$l_value_out")"
        if grep -q '^net.ipv6.' <<< "$l_parameter_name"; then
            [ -z "$l_ipv6_disabled" ] && f_ipv6_chk
            if [ "$l_ipv6_disabled" = "yes" ]; then
                a_output+=(" - IPv6 is disabled on the system,
\"$l_parameter_name\" is not applicable")
            else
                f_kernel_parameter_chk
            fi
        else
            f_kernel_parameter_chk
        fi
    done < <(printf '%s\\n' "${a_parlist[@]})"
    if [ "${#a_output2[@]}" -le 0 ]; then
        printf '%s\\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
    else
        printf '%s\\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
        [ "${#a_output2[@]}" -gt 0 ] && printf '%s\\n' "" "- Correctly set:"
"${a_output[@]}" ""
    fi
}

```

## Remediation:

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv4.icmp_ignore_bogus_error_responses = 1`

### Example:

```
# printf '%s\n' "net.ipv4.icmp_ignore_bogus_error_responses = 1" >>
/etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

```
#!/usr/bin/env bash

{
    sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1
    sysctl -w net.ipv4.route.flush=1
}
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

### Default Value:

`net.ipv4.icmp_ignore_bogus_error_responses = 1`

### References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                 | IG 3                                                                                 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |   |   |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0040  | M1053       |

### 3.3.4 Ensure broadcast icmp requests are ignored (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

Setting `net.ipv4.icmp_echo_ignore_broadcasts` to `1` will cause the system to ignore all ICMP echo and timestamp requests to broadcast and multicast addresses.

#### Rationale:

Accepting ICMP echo and timestamp requests with broadcast or multicast destinations for your network could be used to trick your host into starting (or participating) in a Smurf attack. A Smurf attack relies on an attacker sending large amounts of ICMP broadcast messages with a spoofed source address. All hosts receiving this message and responding would send echo-reply messages back to the spoofed address, which is probably not routable. If many hosts respond to the packets, the amount of traffic on the network could be significantly multiplied.

#### Audit:

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.icmp_echo_ignore_broadcasts` is set to `1`

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); l_ipv6_disabled=""
    a_parlist=("net.ipv4.icmp_echo_ignore_broadcasts=1")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    f_ipv6_chk()
    {
        l_ipv6_disabled="no"
        ! grep -Pqs -- '^\h*0\b' /sys/module/ipv6/parameters/disable &&
l_ipv6_disabled="yes"
        if sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs --
"^\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\b" && \
            sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs --
"^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\b"; then
            l_ipv6_disabled="yes"
        fi
    }
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F=
'{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\"")
            "        in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"") \
            "        in the running configuration" \
            "        and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="$l_out//# /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_file")
                fi
            fi
            done < <("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([\^#\n\r]+|[\^#\n\r\/[\^#\n\r\h]+\.\conf\b)')
            if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
                l_kpar="$(grep -Po "^\h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
                l_kpar="$l_kpar//\./}"
                [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_ufwscf")
            fi
            if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
                while IFS="=" read -r l_fkpname l_file_parameter_value; do

```



```

        l_fkpname="${l_fkpname// /}";
l_file_parameter_value="${l_file_parameter_value// /}"
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_file_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\" \" \" \
                " in \"$(printf '%s' "${A_out[@]})\" \" \"")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\" \" \" \
                " in \"$(printf '%s' "${A_out[@]})\" \" \" \" \
                " and should have a value of: \"$l_value_out\" \" \"")
        fi
        done < <(grep -Po -- "^\\h*$l_parameter_name\\h*=\\h*\\H+"
"${A_out[@]})"
        else
            a_output2+=(" - \"$l_parameter_name\" is not set in an included
file\" \" \
                " ** Note: \"$l_parameter_name\" May be set in a file that's
ignored by load procedure **")
        fi
    }
    l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
    while IFS="=" read -r l_parameter_name l_parameter_value; do # Assess and
check parameters
        l_parameter_name="${l_parameter_name// /}";
l_parameter_value="${l_parameter_value// /}"
        l_value_out="${l_parameter_value//-/ through }";
l_value_out="${l_value_out//|/ or }"
        l_value_out="$(tr -d '()' {} <<< "$l_value_out")"
        if grep -q '^net.ipv6.' <<< "$l_parameter_name"; then
            [ -z "$l_ipv6_disabled" ] && f_ipv6_chk
            if [ "$l_ipv6_disabled" = "yes" ]; then
                a_output+=(" - IPv6 is disabled on the system,
\"$l_parameter_name\" is not applicable")
            else
                f_kernel_parameter_chk
            fi
        else
            f_kernel_parameter_chk
        fi
        done < <(printf '%s\\n' "${a_parlist[@]})"
        if [ "${#a_output2[@]}" -le 0 ]; then
            printf '%s\\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
        else
            printf '%s\\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
            [ "${#a_output2[@]}" -gt 0 ] && printf '%s\\n' "" "- Correctly set:"
"${a_output[@]}" ""
        fi
    }
}

```

## Remediation:

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv4.icmp_echo_ignore_broadcasts = 1`

### Example:

```
# printf '%s\n' "net.ipv4.icmp_echo_ignore_broadcasts = 1" >>
/etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

```
#!/usr/bin/env bash

{
    sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
    sysctl -w net.ipv4.route.flush=1
}
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

### Default Value:

`net.ipv4.icmp_echo_ignore_broadcasts = 1`

### References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230537  
Rule ID: SV-230537r858797  
STIG ID: RHEL-08-040230  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      | ●    | ●    |
| v7               | <u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1498, T1498.001            | TA0040  | M1037       |

### 3.3.5 Ensure icmp redirects are not accepted (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables.

#### Rationale:

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables. By setting `net.ipv4.conf.all.accept_redirects`, `net.ipv4.conf.default.accept_redirects`, `net.ipv6.conf.all.accept_redirects`, and `net.ipv6.conf.default.accept_redirects` to `0`, the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

#### Audit:

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.conf.all.accept_redirects` is set to `0`
- `net.ipv4.conf.default.accept_redirects` is set to `0`
- `net.ipv6.conf.all.accept_redirects` is set to `0`
- `net.ipv6.conf.default.accept_redirects` is set to `0`

#### Note:

- kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.
- IPv6 kernel parameters only apply to systems where IPv6 is enabled

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); l_ipv6_disabled=""
    a_parlist=("net.ipv4.conf.all.accept_redirects=0"
"net.ipv4.conf.default.accept_redirects=0"
"net.ipv6.conf.all.accept_redirects=0"
"net.ipv6.conf.default.accept_redirects=0")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    f_ipv6_chk()
    {
        l_ipv6_disabled="no"
        ! grep -Pqs -- '^\h*0\b' /sys/module/ipv6/parameters/disable &&
l_ipv6_disabled="yes"
        if sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs --
"^\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\b" && \
            sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs --
"^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\b"; then
            l_ipv6_disabled="yes"
        fi
    }
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F=
'{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\"")
            "    in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"") \
            "    in the running configuration" \
            "    and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="$l_out//# /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_file")
                fi
            fi
        done < ("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([\^#\n\r]+|\#\h*\[/\^#\n\r\h]+\.\conf\b)')
        if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
            l_kpar="$(grep -Po "^\h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
            l_kpar="$l_kpar//\./."
            [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_ufwscf")
        fi
    }
}

```

```

        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
        while IFS="" read -r l_fkpname l_file_parameter_value; do
            l_fkpname="${l_fkpname// /}";
l_file_parameter_value="${l_file_parameter_value// /}"
            if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_file_parameter_value"; then
                a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\" \" \" \
                "      in \"$(printf '%s' "${A_out[@]}")\" \" \" )
            else
                a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\" \" \" \
                "      in \"$(printf '%s' "${A_out[@]}")\" \" \" \
                "      and should have a value of: \"$l_value_out\" \" \" )
            fi
        done < <(grep -Po -- "^\\h*$l_parameter_name\\h*=\\h*\\H+"
"${A_out[@]}")
        else
            a_output2+=(" - \"$l_parameter_name\" is not set in an included
file\" \" \
            "      ** Note: \"$l_parameter_name\" May be set in a file that's
ignored by load procedure **\" )
        fi
    }
    l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
    while IFS="" read -r l_parameter_name l_parameter_value; do # Assess and
check parameters
        l_parameter_name="${l_parameter_name// /}";
l_parameter_value="${l_parameter_value// /}"
        l_value_out="${l_parameter_value//-/ through }";
l_value_out="${l_value_out//|/ or }"
        l_value_out="$(tr -d '(){}' <<< "$l_value_out")"
        if grep -q '^net.ipv6.' <<< "$l_parameter_name"; then
            [ -z "$l_ipv6_disabled" ] && f_ipv6_chk
            if [ "$l_ipv6_disabled" = "yes" ]; then
                a_output+=(" - IPv6 is disabled on the system,
\"$l_parameter_name\" is not applicable")
            else
                f_kernel_parameter_chk
            fi
        else
            f_kernel_parameter_chk
        fi
    done < <(printf '%s\\n' "${a_parlist[@]}")
    if [ "${#a_output2[@]}" -le 0 ]; then
        printf '%s\\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
    else
        printf '%s\\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
        [ "${#a_output[@]}" -gt 0 ] && printf '%s\\n' "" "- Correctly set:"
"${a_output[@]}" ""
    fi
}

```

## Remediation:

Set the following parameters in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv4.conf.all.accept_redirects = 0`
- `net.ipv4.conf.default.accept_redirects = 0`

### Example:

```
# printf '%s\n' "net.ipv4.conf.all.accept_redirects = 0"
"net.ipv4.conf.default.accept_redirects = 0" >> /etc/sysctl.d/60-
netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

```
#!/usr/bin/env bash

{
    sysctl -w net.ipv4.conf.all.accept_redirects=0
    sysctl -w net.ipv4.conf.default.accept_redirects=0
    sysctl -w net.ipv4.route.flush=1
}
```

- IF - IPv6 is enabled on the system:

Set the following parameters in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv6.conf.all.accept_redirects = 0`
- `net.ipv6.conf.default.accept_redirects = 0`

### Example:

```
# printf '%s\n' "net.ipv6.conf.all.accept_redirects = 0"
"net.ipv6.conf.default.accept_redirects = 0" >> /etc/sysctl.d/60-
netipv6_sysctl.conf
```

Run the following script to set the active kernel parameters:

```
#!/usr/bin/env bash

{
    sysctl -w net.ipv6.conf.all.accept_redirects=0
    sysctl -w net.ipv6.conf.default.accept_redirects=0
    sysctl -w net.ipv6.route.flush=1
}
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

**Default Value:**

net.ipv4.conf.all.accept\_redirects = 1

net.ipv4.conf.default.accept\_redirects = 1

net.ipv6.conf.all.accept\_redirects = 1

net.ipv6.conf.default.accept\_redirects = 1

**References:**

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

**Additional Information:**

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`



GROUP ID: V-230535  
RULE ID: SV-230535r858793  
STIG ID: RHEL-08-040210  
SEVERITY: CAT II

GROUP ID: V-230544  
RULE ID: SV-230544r858820  
STIG ID: RHEL-08-040280  
SEVERITY: CAT II

GROUP ID: V-230550  
RULE ID: SV-230550r627750  
STIG ID: RHEL-08-040290  
SEVERITY: CAT II

GROUP ID: V-230553  
RULE ID: SV-230553r809324  
STIG ID: RHEL-08-040320  
SEVERITY: CAT II

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics        | Mitigations  |
|-----------------------------|----------------|--------------|
| T1557, T1557.000            | TA0006, TA0009 | M1030, M1042 |

### 3.3.6 Ensure secure icmp redirects are not accepted (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

Secure ICMP redirects are the same as ICMP redirects, except they come from gateways listed on the default gateway list. It is assumed that these gateways are known to your system, and that they are likely to be secure.

#### Rationale:

It is still possible for even known gateways to be compromised. Setting `net.ipv4.conf.all.secure_redirects` and `net.ipv4.conf.default.secure_redirects` to `0` protects the system from routing table updates by possibly compromised known gateways.

#### Audit:

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.conf.all.secure_redirects` is set to `0`
- `net.ipv4.conf.default.secure_redirects` is set to `0`

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); l_ipv6_disabled=""
    a_parlist=("net.ipv4.conf.all.secure_redirects=0"
"net.ipv4.conf.default.secure_redirects=0")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print
$2}' /etc/default/ufw)"
    f_ipv6_chk()
    {
        l_ipv6_disabled="no"
        ! grep -Pqs -- '^h*0\b' /sys/module/ipv6/parameters/disable &&
l_ipv6_disabled="yes"
        if sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs --
"^h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\b" && \
            sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs --
"^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\b"; then
            l_ipv6_disabled="yes"
        fi
    }
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F=
'{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\""
                " in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"" \
                " in the running configuration" \
                " and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//# /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ] = "$l_file")
                fi
            fi
            done < <("$l_systemdsysctl" --cat-config | grep -Po
'^h*(\[\^#\n\r]+|\#\h*\[/\^#\n\r\h]+\.\conf\b)')
            if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
                l_kpar="$(grep -Po "^h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
                l_kpar="${l_kpar//\\/\\.}"
                [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ] = "$l_ufwscf")
            fi
            if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output

```

```

while IFS="" read -r l_fkpname l_file_parameter_value; do
    l_fkpname="${l_fkpname// /}";
l_file_parameter_value="${l_file_parameter_value// /}"
    if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_file_parameter_value"; then
        a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\"" \
            "      in \"$(printf '%s' "${A_out[@]}")\"")
    else
        a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\"" \
            "      in \"$(printf '%s' "${A_out[@]}")\" " \
            "      and should have a value of: \"$l_value_out\"")
    fi
done < <(grep -Po -- "^\\h*$l_parameter_name\\h*=\\h*\\H+"
"${A_out[@]}")
else
    a_output2+=(" - \"$l_parameter_name\" is not set in an included
file" \
        "      ** Note: \"$l_parameter_name\" May be set in a file that's
ignored by load procedure **")
fi
}
l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
while IFS="" read -r l_parameter_name l_parameter_value; do # Assess and
check parameters
    l_parameter_name="${l_parameter_name// /}";
l_parameter_value="${l_parameter_value// /}"
    l_value_out="${l_parameter_value//-/ through }";
l_value_out="${l_value_out//|/ or }"
    l_value_out="$(tr -d '(){}' <<< "$l_value_out")"
    if grep -q '^net.ipv6.' <<< "$l_parameter_name"; then
        [ -z "$l_ipv6_disabled" ] && f_ipv6_chk
        if [ "$l_ipv6_disabled" = "yes" ]; then
            a_output+=(" - IPv6 is disabled on the system,
\"$l_parameter_name\" is not applicable")
        else
            f_kernel_parameter_chk
        fi
    else
        f_kernel_parameter_chk
    fi
done < <(printf '%s\\n' "${a_parlist[@]}")
if [ "${#a_output2[@]}" -le 0 ]; then
    printf '%s\\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
else
    printf '%s\\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
    [ "${#a_output2[@]}" -gt 0 ] && printf '%s\\n' "" "- Correctly set:"
"${a_output[@]}" ""
fi
}

```

## Remediation:

Set the following parameters in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv4.conf.all.secure_redirects = 0`
- `net.ipv4.conf.default.secure_redirects = 0`

### Example:

```
# printf '%s\n' "net.ipv4.conf.all.secure_redirects = 0"
"net.ipv4.conf.default.secure_redirects = 0" >> /etc/sysctl.d/60-
netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

```
#!/usr/bin/env bash

{
    sysctl -w net.ipv4.conf.all.secure_redirects=0
    sysctl -w net.ipv4.conf.default.secure_redirects=0
    sysctl -w net.ipv4.route.flush=1
}
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## Default Value:

`net.ipv4.conf.all.secure_redirects = 1`

`net.ipv4.conf.default.secure_redirects = 1`

## References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics        | Mitigations  |
|-----------------------------|----------------|--------------|
| T1557, T1557.000            | TA0006, TA0009 | M1030, M1042 |

### 3.3.7 Ensure reverse path filtering is enabled (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

Setting `net.ipv4.conf.all.rp_filter` and `net.ipv4.conf.default.rp_filter` to `1` forces the Linux kernel to utilize reverse path filtering on a received packet to determine if the packet was valid. Essentially, with reverse path filtering, if the return packet does not go out the same interface that the corresponding source packet came from, the packet is dropped (and logged if `log_martians` is set).

#### Rationale:

Setting `net.ipv4.conf.all.rp_filter` and `net.ipv4.conf.default.rp_filter` to `1` is a good way to deter attackers from sending your system bogus packets that cannot be responded to. One instance where this feature breaks down is if asymmetrical routing is employed. This would occur when using dynamic routing protocols (bgp, ospf, etc) on your system. If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

#### Impact:

If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

#### Audit:

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.conf.all.rp_filter` is set to `1`
- `net.ipv4.conf.default.rp_filter` is set to `1`

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); l_ipv6_disabled=""
    a_parlist=("net.ipv4.conf.all.rp_filter=1"
"net.ipv4.conf.default.rp_filter=1")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    f_ipv6_chk()
    {
        l_ipv6_disabled="no"
        ! grep -Pqs -- '^\h*0\b' /sys/module/ipv6/parameters/disable &&
l_ipv6_disabled="yes"
        if sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs --
"^\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\b" && \
            sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs --
"^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\b"; then
            l_ipv6_disabled="yes"
        fi
    }
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F=
'{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\""
                " in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"" \
                " in the running configuration" \
                " and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//# /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=(["$l_kpar"]="${l_file}")
                fi
            fi
        done < <("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([\h*\n\r]+|\h*\n\r/[\h*\n\r\h]+\.\conf\b)')
        if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
            l_kpar="$(grep -Po "^\h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
            l_kpar="${l_kpar//\./}"
            [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=(["$l_kpar"]="${l_ufwscf}")
        fi
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output

```





## Remediation:

Set the following parameters in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv4.conf.all.rp_filter = 1`
- `net.ipv4.conf.default.rp_filter = 1`

### Example:

```
# printf '%s\n' "net.ipv4.conf.all.rp_filter = 1"
"net.ipv4.conf.default.rp_filter = 1" >> /etc/sysctl.d/60-netip4_sysctl.conf
```

Run the following script to set the active kernel parameters:

```
#!/usr/bin/env bash

{
    sysctl -w net.ipv4.conf.all.rp_filter=1
    sysctl -w net.ipv4.conf.default.rp_filter=1
    sysctl -w net.ipv4.route.flush=1
}
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

### Default Value:

`net.ipv4.conf.all.rp_filter = 2`

`net.ipv4.conf.default.rp_filter = 1`

### References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230549  
Rule ID: SV-230549r858830  
STIG ID: RHEL-08-040285  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      | ●    | ●    |
| v7               | <u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics        | Mitigations  |
|-----------------------------|----------------|--------------|
| T1498, T1498.001            | TA0006, TA0040 | M1030, M1042 |

### *3.3.8 Ensure source routed packets are not accepted (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### **Description:**

In networking, source routing allows a sender to partially or fully specify the route packets take through a network. In contrast, non-source routed packets travel a path determined by routers in the network. In some cases, systems may not be routable or reachable from some locations (e.g. private addresses vs. Internet routable), and so source routed packets would need to be used.

#### **Rationale:**

Setting `net.ipv4.conf.all.accept_source_route`, `net.ipv4.conf.default.accept_source_route`, `net.ipv6.conf.all.accept_source_route` and `net.ipv6.conf.default.accept_source_route` to `0` disables the system from accepting source routed packets. Assume this system was capable of routing packets to Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

**Audit:**

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.conf.all.accept_source_route` is set to 0
- `net.ipv4.conf.default.accept_source_route` is set to 0
- `net.ipv6.conf.all.accept_source_route` is set to 0
- `net.ipv6.conf.default.accept_source_route` is set to 0

**Note:**

- kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.
- IPv6 kernel parameters only apply to systems where IPv6 is enabled

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); l_ipv6_disabled=""
    a_parlist=("net.ipv4.conf.all.accept_source_route=0"
"net.ipv4.conf.default.accept_source_route=0"
"net.ipv6.conf.all.accept_source_route=0"
"net.ipv6.conf.default.accept_source_route=0")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    f_ipv6_chk()
    {
        l_ipv6_disabled="no"
        ! grep -Pqs -- '^\h*0\b' /sys/module/ipv6/parameters/disable &&
l_ipv6_disabled="yes"
        if sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs --
"^\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\b" && \
            sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs --
"^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\b"; then
            l_ipv6_disabled="yes"
        fi
    }
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F=
'{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\"")
            "    in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"") \
            "    in the running configuration" \
            "    and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="$l_out//# /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_file")
                fi
            fi
        done < ("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([\^#\n\r]+|#[\h*\[/\^#\n\r\h]+\.\conf\b)')
        if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
            l_kpar="$(grep -Po "^\h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
            l_kpar="$l_kpar//\./."
            [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_ufwscf")
        fi
    }
}

```



## Remediation:

Set the following parameters in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv4.conf.all.accept_source_route = 0`
- `net.ipv4.conf.default.accept_source_route = 0`

### Example:

```
# printf '%s\n' "net.ipv4.conf.all.accept_source_route = 0"
"net.ipv4.conf.default.accept_source_route = 0" >> /etc/sysctl.d/60-
netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

```
#!/usr/bin/env bash

{
    sysctl -w net.ipv4.conf.all.accept_source_route=0
    sysctl -w net.ipv4.conf.default.accept_source_route=0
    sysctl -w net.ipv4.route.flush=1
}
```

- IF - IPv6 is enabled on the system:

Set the following parameters in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv6.conf.all.accept_source_route = 0`
- `net.ipv6.conf.default.accept_source_route = 0`

### Example:

```
# printf '%s\n' "net.ipv6.conf.all.accept_source_route = 0"
"net.ipv6.conf.default.accept_source_route = 0" >> /etc/sysctl.d/60-
netipv6_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
#!/usr/bin/env bash

{
    sysctl -w net.ipv6.conf.all.accept_source_route=0
    sysctl -w net.ipv6.conf.default.accept_source_route=0
    sysctl -w net.ipv6.route.flush=1
}
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten



**Default Value:**

net.ipv4.conf.all.accept\_source\_route = 0

net.ipv4.conf.default.accept\_source\_route = 0

net.ipv6.conf.all.accept\_source\_route = 0

net.ipv6.conf.default.accept\_source\_route = 0

**References:**

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

**Additional Information:**

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

GROUP ID: V-230538  
RULE ID: SV-230538r858801  
STIG ID: RHEL-08-040240  
SEVERITY: CAT II

GROUP ID: V-230539  
RULE ID: SV-230539r861085  
STIG ID: RHEL-08-040250  
SEVERITY: CAT II

GROUP ID: V-230541  
RULE ID: SV-230541r858812  
STIG ID: RHEL-08-040261  
SEVERITY: CAT II

GROUP ID: V-230542  
RULE ID: SV-230542r858814  
STIG ID: RHEL-08-040262  
SEVERITY: CAT II

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1590, T1590.005            | TA0007  |             |

### 3.3.9 *Ensure suspicious packets are logged (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

When enabled, this feature logs packets with un-routable source addresses to the kernel log.

#### **Rationale:**

Setting `net.ipv4.conf.all.log_martians` and `net.ipv4.conf.default.log_martians` to `1` enables this feature. Logging these packets allows an administrator to investigate the possibility that an attacker is sending spoofed packets to their system.

#### **Audit:**

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.conf.all.log_martians` is set to `1`
- `net.ipv4.conf.default.log_martians` is set to `1`

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); l_ipv6_disabled=""
    a_parlist=("net.ipv4.conf.all.log_martians=1"
"net.ipv4.conf.default.log_martians=1")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print
$2}' /etc/default/ufw)"
    f_ipv6_chk()
    {
        l_ipv6_disabled="no"
        ! grep -Pqs -- '^\h*0\b' /sys/module/ipv6/parameters/disable &&
l_ipv6_disabled="yes"
        if sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs --
"^\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\b" && \
            sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs --
"^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\b"; then
            l_ipv6_disabled="yes"
        fi
    }
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F=
'{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\""
                " in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"" \
                " in the running configuration" \
                " and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//# /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_file")
                fi
            fi
            done < <("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([\h*\n\r]+|[\h*\n\r\h]+\.\conf\b)')
            if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
                l_kpar="$(grep -Po "^\h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
                l_kpar="${l_kpar//\./}"
                [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_ufwscf")
            fi
            if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output

```

```

        while IFS="" read -r l_fkpname l_file_parameter_value; do
            l_fkpname="${l_fkpname// /}";
l_file_parameter_value="${l_file_parameter_value// /}"
            if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_file_parameter_value"; then
                a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\" \" \" \
                "      in \"$(printf '%s' "${A_out[@]}")\" \" \" )
            else
                a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\" \" \" \
                "      in \"$(printf '%s' "${A_out[@]}")\" \" \" \
                "      and should have a value of: \"$l_value_out\" \" \" )
            fi
        done < <(grep -Po -- "^\\h*$l_parameter_name\\h*=\\h*\\H+"
"${A_out[@]}")
        else
            a_output2+=(" - \"$l_parameter_name\" is not set in an included
file\" \" \
            "      ** Note: \"$l_parameter_name\" May be set in a file that's
ignored by load procedure **\" )
        fi
    }
    l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
    while IFS="" read -r l_parameter_name l_parameter_value; do # Assess and
check parameters
        l_parameter_name="${l_parameter_name// /}";
l_parameter_value="${l_parameter_value// /}"
        l_value_out="${l_parameter_value//-/ through }";
l_value_out="${l_value_out//|/ or }"
        l_value_out="$(tr -d '(){}' <<< "$l_value_out")"
        if grep -q '^net.ipv6.' <<< "$l_parameter_name"; then
            [ -z "$l_ipv6_disabled" ] && f_ipv6_chk
            if [ "$l_ipv6_disabled" = "yes" ]; then
                a_output+=(" - IPv6 is disabled on the system,
\"$l_parameter_name\" is not applicable")
            else
                f_kernel_parameter_chk
            fi
        else
            f_kernel_parameter_chk
        fi
    done < <(printf '%s\\n' "${a_parlist[@]}")
    if [ "${#a_output2[@]}" -le 0 ]; then
        printf '%s\\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
    else
        printf '%s\\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
        [ "${#a_output[@]}" -gt 0 ] && printf '%s\\n' "" "- Correctly set:"
"${a_output[@]}" ""
    fi
}

```

## Remediation:

Set the following parameters in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv4.conf.all.log_martians = 1`
- `net.ipv4.conf.default.log_martians = 1`

### Example:

```
# printf '%s\n' "net.ipv4.conf.all.log_martians = 1"
"net.ipv4.conf.default.log_martians = 1" >> /etc/sysctl.d/60-
netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

```
#!/usr/bin/env bash

{
    sysctl -w net.ipv4.conf.all.log_martians=1
    sysctl -w net.ipv4.conf.default.log_martians=1
    sysctl -w net.ipv4.route.flush=1
}
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

## Default Value:

`net.ipv4.conf.all.log_martians = 0`

`net.ipv4.conf.default.log_martians = 0`

## References:

1. NIST SP 800-53 Rev. 5: AU-3

## Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |                                                                                     |  |  |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         |  |  |  |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.                                                                                |                                                                                     |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0005  |             |

### 3.3.10 Ensure tcp syn cookies is enabled (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

When `tcp_syncookies` is set, the kernel will handle TCP SYN packets normally until the half-open connection queue is full, at which time, the SYN cookie functionality kicks in. SYN cookies work by not using the SYN queue at all. Instead, the kernel simply replies to the SYN with a SYN/ACK, but will include a specially crafted TCP sequence number that encodes the source and destination IP address and port number and the time the packet was sent. A legitimate connection would send the ACK packet of the three way handshake with the specially crafted sequence number. This allows the system to verify that it has received a valid response to a SYN cookie and allow the connection, even though there is no corresponding SYN in the queue.

#### Rationale:

Attackers use SYN flood attacks to perform a denial of service attack on a system by sending many SYN packets without completing the three way handshake. This will quickly use up slots in the kernel's half-open connection queue and prevent legitimate connections from succeeding. Setting `net.ipv4.tcp_syncookies` to `1` enables SYN cookies, allowing the system to keep accepting valid connections, even if under a denial of service attack.

#### Audit:

Run the following script to verify the following kernel parameter is set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv4.tcp_syncookies` is set to `1`

**Note:** kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.



```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); l_ipv6_disabled=""
    a_parlist=("net.ipv4.tcp_syncookies=1")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    f_ipv6_chk()
    {
        l_ipv6_disabled="no"
        ! grep -Pqs -- '^\h*0\b' /sys/module/ipv6/parameters/disable &&
l_ipv6_disabled="yes"
        if sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs --
"^\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\b" && \
            sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs --
"^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\b"; then
            l_ipv6_disabled="yes"
        fi
    }
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F=
'{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\"")
            "    in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"") \
            "    in the running configuration" \
            "    and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="$l_out//# /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_file")
                fi
            fi
            done < <("$l_systemdsysctl" --cat-config | grep -Po
'^\h*([\^#\n\r]+|[\^#\h*\n\r\h]+\.\conf\b)')
            if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
                l_kpar="$(grep -Po "^\h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
                l_kpar="$l_kpar//.}"
                [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ]="$l_ufwscf")
            fi
            if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output
                while IFS="=" read -r l_fkpname l_file_parameter_value; do

```

```

        l_fkpname="${l_fkpname// /}";
l_file_parameter_value="${l_file_parameter_value// /}"
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_file_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\" \" \" \
                "      in \"$(printf '%s' "${A_out[@]})\" \" \"")
            else
                a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\" \" \" \
                "      in \"$(printf '%s' "${A_out[@]})\" \" \" \" \
                "      and should have a value of: \"$l_value_out\" \" \"")
            fi
        done < <(grep -Po -- "^\\h*$l_parameter_name\\h*=\\h*\\H+"
"${A_out[@]})"
        else
            a_output2+=(" - \"$l_parameter_name\" is not set in an included
file\" \" \
                "      ** Note: \"$l_parameter_name\" May be set in a file that's
ignored by load procedure **")
        fi
    }
    l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
    while IFS="" read -r l_parameter_name l_parameter_value; do # Assess and
check parameters
        l_parameter_name="${l_parameter_name// /}";
l_parameter_value="${l_parameter_value// /}"
        l_value_out="${l_parameter_value//-/ through }";
l_value_out="${l_value_out//|/ or }"
        l_value_out="$(tr -d '()' {} <<< "$l_value_out")"
        if grep -q '^net.ipv6.' <<< "$l_parameter_name"; then
            [ -z "$l_ipv6_disabled" ] && f_ipv6_chk
            if [ "$l_ipv6_disabled" = "yes" ]; then
                a_output+=(" - IPv6 is disabled on the system,
\"$l_parameter_name\" is not applicable")
            else
                f_kernel_parameter_chk
            fi
        else
            f_kernel_parameter_chk
        fi
    done < <(printf '%s\\n' "${a_parlist[@]})"
    if [ "${#a_output2[@]}" -le 0 ]; then
        printf '%s\\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
    else
        printf '%s\\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
        [ "${#a_output2[@]}" -gt 0 ] && printf '%s\\n' "" "- Correctly set:"
"${a_output[@]}" ""
    fi
}

```

## Remediation:

Set the following parameter in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv4.tcp_syncookies = 1`

### Example:

```
# printf '%s\n' "net.ipv4.tcp_syncookies = 1" >> /etc/sysctl.d/60-netip4_sysctl.conf
```

Run the following script to set the active kernel parameters:

```
#!/usr/bin/env bash

{
    sysctl -w net.ipv4.tcp_syncookies=1
    sysctl -w net.ipv4.route.flush=1
}
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

### Default Value:

`net.ipv4.tcp_syncookies = 1`

### References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

### Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1499, T1499.001            | TA0040  | M1037       |

### 3.3.11 Ensure ipv6 router advertisements are not accepted (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

Routers periodically multicast Router Advertisement messages to announce their availability and convey information to neighboring nodes that enable them to be automatically configured on the network.

`net.ipv6.conf.all.accept_ra` and `net.ipv6.conf.default.accept_ra` determine the systems ability to accept these advertisements

#### Rationale:

It is recommended that systems do not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes. Setting `net.ipv6.conf.all.accept_ra` and `net.ipv6.conf.default.accept_ra` to `0` disables the system's ability to accept IPv6 router advertisements.

#### Audit:

Run the following script to verify the following kernel parameters are set in the running configuration and correctly loaded from a kernel parameter configuration file:

- `net.ipv6.conf.all.accept_ra` is set to `0`
- `net.ipv6.conf.default.accept_ra` is set to `0`

#### Note:

- kernel parameters are loaded by file and parameter order precedence. The following script observes this precedence as part of the auditing procedure. The parameters being checked may be set correctly in a file. If that file is superseded, the parameter is overridden by an incorrect setting later in that file, or in a canonically later file, that "correct" setting will be ignored both by the script and by the system during a normal kernel parameter load sequence.
- IPv6 kernel parameters only apply to systems where IPv6 is enabled

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=(); l_ipv6_disabled=""
    a_parlist=("net.ipv6.conf.all.accept_ra=0"
"net.ipv6.conf.default.accept_ra=0")
    l_ufwscf="$([ -f /etc/default/ufw ] && awk -F= '/^\s*IPT_SYSCTL=/ {print $2}' /etc/default/ufw)"
    f_ipv6_chk()
    {
        l_ipv6_disabled="no"
        ! grep -Pqs -- '^h*0\b' /sys/module/ipv6/parameters/disable &&
l_ipv6_disabled="yes"
        if sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs --
"^h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\b" && \
            sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs --
"^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\b"; then
            l_ipv6_disabled="yes"
        fi
    }
    f_kernel_parameter_chk()
    {
        l_running_parameter_value="$(sysctl "$l_parameter_name" | awk -F=
'{print $2}' | xargs)" # Check running configuration
        if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_running_parameter_value"; then
            a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_running_parameter_value\"
"          in the running configuration")
        else
            a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_running_parameter_value\"
"          in the running configuration" \
"          and should have a value of: \"$l_value_out\"")
        fi
        unset A_out; declare -A A_out # Check durable setting (files)
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//# /}"
                else
                    l_kpar="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ] = "$l_file")
                fi
            fi
        done < <("$l_systemdsysctl" --cat-config | grep -Po
'^h*(\[\^#\n\r\]|#\h*\[/\^#\n\r\h]+\.\conf\b)')
        if [ -n "$l_ufwscf" ]; then # Account for systems with UFW (Not covered
by systemd-sysctl --cat-config)
            l_kpar="$(grep -Po "^h*$l_parameter_name\b" "$l_ufwscf" | xargs)"
            l_kpar="${l_kpar//\./}"
            [ "$l_kpar" = "$l_parameter_name" ] &&
A_out+=([ "$l_kpar" ] = "$l_ufwscf")
        fi
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate
output

```

```

        while IFS="" read -r l_fkpname l_file_parameter_value; do
            l_fkpname="${l_fkpname// /}";
            l_file_parameter_value="${l_file_parameter_value// /}"
            if grep -Pq -- '\b'"$l_parameter_value"' \b' <<<
"$l_file_parameter_value"; then
                a_output+=(" - \"$l_parameter_name\" is correctly set to
\"$l_file_parameter_value\" \" \" \
                "      in \"$(printf '%s' "${A_out[@]})\" \" \"")
            else
                a_output2+=(" - \"$l_parameter_name\" is incorrectly set to
\"$l_file_parameter_value\" \" \" \
                "      in \"$(printf '%s' "${A_out[@]})\" \" \" \" \
                "      and should have a value of: \"$l_value_out\" \" \"")
            fi
            done < <(grep -Po -- "^\\h*$l_parameter_name\\h*=\\h*\\H+"
"$${A_out[@]}")
            else
                a_output2+=(" - \"$l_parameter_name\" is not set in an included
file\" \" \
                "      ** Note: \"$l_parameter_name\" May be set in a file that's
ignored by load procedure **")
            fi
        }
        l_systemdsysctl="$(readlink -f /lib/systemd/systemd-sysctl)"
        while IFS="" read -r l_parameter_name l_parameter_value; do # Assess and
check parameters
            l_parameter_name="${l_parameter_name// /}";
            l_parameter_value="${l_parameter_value// /}"
            l_value_out="${l_parameter_value//-/ through }";
            l_value_out="${l_value_out//|/ or }"
            l_value_out="$(tr -d '(){}' <<< "$l_value_out")"
            if grep -q '^net.ipv6.' <<< "$l_parameter_name"; then
                [ -z "$l_ipv6_disabled" ] && f_ipv6_chk
                if [ "$l_ipv6_disabled" = "yes" ]; then
                    a_output+=(" - IPv6 is disabled on the system,
\"$l_parameter_name\" is not applicable")
                else
                    f_kernel_parameter_chk
                fi
            else
                f_kernel_parameter_chk
            fi
            done < <(printf '%s\\n' "${a_parlist[@]}")
            if [ "${#a_output2[@]}" -le 0 ]; then
                printf '%s\\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
            else
                printf '%s\\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
                [ "${#a_output2[@]}" -gt 0 ] && printf '%s\\n' "" "- Correctly set:"
"${a_output[@]}" ""
            fi
        }
    }

```

## Remediation:

- **IF** - IPv6 is enabled on the system:

Set the following parameters in `/etc/sysctl.conf` or a file in `/etc/sysctl.d/` ending in `.conf`:

- `net.ipv6.conf.all.accept_ra = 0`
- `net.ipv6.conf.default.accept_ra = 0`

### Example:

```
# printf '%s\n' "net.ipv6.conf.all.accept_ra = 0"
"net.ipv6.conf.default.accept_ra = 0" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```

Run the following script to set the active kernel parameters:

```
#!/usr/bin/env bash

{
    sysctl -w net.ipv6.conf.all.accept_ra=0
    sysctl -w net.ipv6.conf.default.accept_ra=0
    sysctl -w net.ipv6.route.flush=1
}
```

**Note:** If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

### Default Value:

`net.ipv6.conf.all.accept_ra = 1`

`net.ipv6.conf.default.accept_ra = 1`

### References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)



## Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230541  
Rule ID: SV-230541r858812  
STIG ID: RHEL-08-040261  
Severity: CAT II

Vul ID: V-230542  
Rule ID: SV-230542r858814  
STIG ID: RHEL-08-040262  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      | ●    | ●    |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics        | Mitigations  |
|-----------------------------|----------------|--------------|
| T1557, T1557.000            | TA0006, TA0040 | M1030, M1042 |

### 3.3.12 *Ensure net.ipv4.conf.all.forwarding is disabled (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The `net.ipv4.ip_forward` and `net.ipv6.conf.all.forwarding` flags are used to tell the system whether it can forward packets or not.

#### **Rationale:**

The Operating System (OS) must not enable IPv4 packet forwarding unless the system is a router.

#### **Impact:**

Routing protocol daemons are typically used on routers to exchange network topology information with other routers. If this software is used when not required, system network information may be unnecessarily transmitted across the network.

The `sysctl --system` command will load settings from all system configuration files. All configuration files are sorted by their filename in lexicographic order, regardless of which of the directories they reside in. If multiple files specify the same option, the entry in the file with the lexicographically latest name will take precedence. Files are read from directories in the following list from top to bottom. Once a file of a given filename is loaded, any file of the same name in subsequent directories is ignored.

`/etc/sysctl.d/.conf` `/run/sysctl.d/.conf` `/usr/local/lib/sysctl.d/.conf` `/usr/lib/sysctl.d/.conf`  
`/lib/sysctl.d/*.conf` `/etc/sysctl.conf`

## Audit:

Verify the OS is not performing IPv4 packet forwarding, unless the system is a router. Check that IPv4 forwarding is disabled using the following command:

```
# sysctl net.ipv4.conf.all.forwarding  
  
net.ipv4.conf.all.forwarding = 0
```

If the IPv4 forwarding value is not "0" and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding. Check that the configuration files are present to enable this network parameter.

```
# grep -r net.ipv4.conf.all.forwarding /run/sysctl.d/*.conf  
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf  
/etc/sysctl.conf /etc/sysctl.d/*.conf  
  
/etc/sysctl.d/99-sysctl.conf: net.ipv4.conf.all.forwarding = 0
```

If "net.ipv4.conf.all.forwarding" is not set to "0", is missing or commented out, this is a finding.

If conflicting results are returned, this is a finding.

## Remediation:

Configure the OS to not allow IPv4 packet forwarding, unless the system is a router. Add or edit the following line in a system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv4.conf.all.forwarding=0
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/*.conf  
/usr/local/lib/sysctl.d/*.conf  
/usr/lib/sysctl.d/*.conf  
/lib/sysctl.d/*.conf  
/etc/sysctl.conf  
/etc/sysctl.d/*.conf
```

Load settings from all system configuration files with the following command:

```
# sysctl --system
```

## Default Value:

```
net.ipv4.conf.all.forwarding = 1
```

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

On systems with Uncomplicated Firewall, additional settings may be configured in `/etc/ufw/sysctl.conf`

- The settings in `/etc/ufw/sysctl.conf` will override settings in `/etc/sysctl.conf`
- This behavior can be changed by updating the `IPT_SYSCTL` parameter in `/etc/default/ufw`

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

GROUP ID: V-250317  
RULE ID: SV-250317r858808  
STIG ID: RHEL-08-040259  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      | ●    | ●    |
| v7               | <u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics        | Mitigations  |
|-----------------------------|----------------|--------------|
| T1557, T1557.000            | TA0006, TA0009 | M1030, M1042 |

### *3.4 Ensure at least two name servers are configured if using DNS resolution (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

For operating systems using DNS resolution, at least two name servers must be configured.

#### **Rationale:**

To provide availability for name resolution services, multiple redundant name servers are mandated. A failure in name resolution could lead to the failure of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.

#### **Audit:**

Determine whether the system is using local or DNS name resolution with the following command:

```
# grep hosts /etc/nsswitch.conf  
  
hosts: files dns
```

If the DNS entry is missing from the host's line in the "/etc/nsswitch.conf" file, the "/etc/resolv.conf" file must be empty.

Verify the "/etc/resolv.conf" file is empty with the following command:

```
# ls -al /etc/resolv.conf  
  
-rw-r--r-- 1 root root 0 Aug 19 08:31 resolv.conf
```

If local host authentication is being used and the "/etc/resolv.conf" file is not empty, this is a finding.

If the DNS entry is found on the host's line of the "/etc/nsswitch.conf" file, verify the operating system is configured to use two or more name servers for DNS resolution. Determine the name servers used by the system with the following command:

```
# grep nameserver /etc/resolv.conf  
  
nameserver 192.168.1.2  
nameserver 192.168.1.3
```

If less than two lines are returned that are not commented out, this is a finding.

## Remediation:

Configure the operating system to use two or more name servers for DNS resolution. By default, "NetworkManager" on RHEL 8 operating systems dynamically updates the /etc/resolv.conf file with the DNS settings from active "NetworkManager" connection profiles. However, this feature can be disabled to allow manual configurations. If manually configuring DNS, edit the "/etc/resolv.conf" file to uncomment or add the two or more "nameserver" option lines with the IP address of local authoritative name servers. If local host resolution is being performed, the "/etc/resolv.conf" file must be empty. An empty "/etc/resolv.conf" file can be created as follows:

```
# echo -n > /etc/resolv.conf
```

## References:

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230316  
Rule ID: SV-230316r627750  
STIG ID: RHEL-08-010680  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

## 4 Host Based Firewall

A Host Based Firewall, on a Linux system, is a set of rules. When a data packet moves into or out of a protected network space, its contents (in particular, information about its origin, target, and the protocol it plans to use) are tested against the firewall rules to see if it should be allowed through

To provide a Host Based Firewall, the Linux kernel includes support for nftables.

- **nftables** - A subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames. nftables is supposed to replace certain parts of Netfilter, while keeping and reusing most of it. nftables utilizes the building blocks of the Netfilter infrastructure, such as the existing hooks into the networking stack, connection tracking system, userspace queueing component, and logging subsystem.

In order to configure firewall rules for nftables, a firewall utility needs to be installed. Guidance has been included for the following firewall utilities:

- **Firewalld** - Provides firewall features by acting as a front-end for the Linux kernel's netfilter framework via the nftables backend. Starting in v0.6.0, Firewalld added support for acting as a front-end for the Linux kernel's netfilter framework via the nftables userspace utility, acting as an alternative to the nft command line program. firewalld supports both IPv4 and IPv6 networks and can administer separate firewall zones with varying degrees of trust as defined in zone profiles.

### Notes:

- Only **one** method should be used to configure a firewall on the system. Use of more than one method could produce unexpected results.
- This section is intended only to ensure the resulting firewall rules are in place, not how they are configured.
- The **ipset** and **iptables-nft** packages have been deprecated in Fedora 34 based Linux distributions. This includes deprecation of nft-variants such as **iptables**, **ip6tables**, **arptables**, and **ebtables** utilities. If you are using any of these tools, for example, because you upgraded from an earlier version, we recommend migrating to the nft command line tool provided by the nftables package.

## 4.1 Configure a firewall utility

In order to configure firewall rules for Netfilter or nftables, a firewall utility needs to be installed. Guidance has been included for the following firewall utilities:

- **Firewalld:**
  - Provides firewall features by acting as a front-end for the Linux kernel's netfilter framework via the nftables userspace utility, acting as an alternative to the nft command line program. firewalld supports both IPv4 and IPv6 networks and can administer separate firewall zones with varying degrees of trust as defined in zone profiles.
  - Use the firewalld utility for simple firewall use cases. The utility is easy to use and covers the typical use cases for these scenarios.
- **NFTables:**
  - Includes the nft utility for configuration of the nftables subsystem of the Linux kernel
  - Use the nftables utility to set up complex and performance critical firewalls, such as for a whole network.

### Notes:

- Only **one** method should be used to configure a firewall on the system. Use of more than one method could produce unexpected results.
- IPTables are deprecated in this release, and not covered in this Benchmark. The iptables utility on Fedora 28/CentOS 8 stream-based Linux distributions uses the nf\_tables kernel API instead of the legacy back end. The nf\_tables API provides backward compatibility so that scripts that use iptables commands still work on Fedora 28 based Linux distributions. For new firewall scripts, it is recommended to use nftables.



## 4.1.1 Configure firewall rules

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames and is the successor to iptables.

**Important:** Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.

**Note:** Only one method should be used to configure a firewall on the system. Use of more than one method could produce unexpected results.

### Firewalld

The following example will create a Firewalld Zone called **securezone** to implement the firewall rules of this section leveraging the firewalld utility included with the firewalld package. This example will open port 22(ssh) from anywhere. Opening service **SSH** should be updated in accordance with local site policy. If another name for the zone is preferred, replace **securezone** with the name to be used.

*Sample securezone zone xml file*

```
<?xml version="1.0" encoding="utf-8"?>
<zone target="DROP">
  <description>For use with CIS Linux Benchmark. You do not trust the other
  computers on networks to not harm your computer. Only selected incoming
  connections are accepted.</description>
  <service name="ssh"/>
  <service name="dhcpv6-client"/>
  <icmp-block name="destination-unreachable"/>
  <icmp-block name="packet-too-big"/>
  <icmp-block name="time-exceeded"/>
  <icmp-block name="parameter-problem"/>
  <icmp-block name="neighbour-advertisement"/>
  <icmp-block name="neighbour-solicitation"/>
  <icmp-block name="router-advertisement"/>
  <icmp-block name="router-solicitation"/>
  <rule family="ipv4">
    <source address="127.0.0.1"/>
    <destination address="127.0.0.1" invert="True"/>
    <drop/>
  </rule>
  <rule family="ipv6">
    <source address="::1"/>
    <destination address="::1" invert="True"/>
    <drop/>
  </rule>
  <icmp-block-inversion/>
</zone>
```

**Note:** To use this zone, save this as **/etc/firewalld/zones/securezone.xml** and run the following commands:

```
# firewall-cmd --reload
# firewall-cmd --permanent --zone=securezone --change-interface={NAME OF
NETWORK INTERFACE}
```

### **NFTables Utility:**

The following will implement the firewall rules of this section leveraging the nftables utility included with the nftables package. This example will open ICMP, IGMP, and port 22(ssh) from anywhere. Opening the ports for ICMP, IGMP, and port 22(ssh) needs to be updated in accordance with local site policy. Allow port 22(ssh) should to be updated to only allow systems requiring ssh connectivity to connect, as per site policy.

Save the script below as `/etc/nftables/nftables.rules`

```
# This nftables.rules config should be saved as /etc/nftables/nftables.rules

# flush nftables ruleset
flush ruleset

# Load nftables ruleset
# nftables config with inet table named filter

table inet filter {
    chain input {
        type filter hook input priority 0; policy drop;

        # early drop invalid packets
        ct state invalid drop

        # allow loopback if not forged
        iif lo accept
        iif != lo ip daddr 127.0.0.1/8 drop
        iif != lo ip6 daddr ::1/128 drop

        # allow connections made by ourselves
        ip protocol tcp ct state established accept
        ip protocol udp ct state established accept

        # allow from anywhere
        ip protocol igmp accept
        tcp dport ssh accept

        # allow some icmp
        icmpv6 type { destination-unreachable, packet-too-big, time-exceeded,
parameter-problem, mld-listener-query, mld-listener-report, mld-listener-
done, nd-router-solicit, nd-router-advert, nd-neighbor-solicit, nd-neighbor-
advert, ind-neighbor-solicit, ind-neighbor-advert, mld2-listener-report }
accept
        icmp type { destination-unreachable, router-advertisement, router-
solicitation, time-exceeded, parameter-problem } accept
    }

    chain forward {
        # drop all forward
        type filter hook forward priority 0; policy drop;
    }

    chain output {
        # can omit this as its accept by default
        type filter hook output priority 0; policy accept;
    }
}
```

Run the following command to load the file into nftables

```
# nft -f /etc/nftables/nftables.rules
```

**Note:** All changes in the nftables subsections are temporary

To make these changes permanent:

Run the following command to create the nftables.rules file

```
nft list ruleset > /etc/nftables/nftables.rules
```

Add the following line to **/etc/sysconfig/nftables.conf**

```
include "/etc/nftables/nftables.rules"
```

#### *4.1.1.1 Ensure nftables base chains exist (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Chains are containers for rules. They exist in two kinds, base chains and regular chains. A base chain is an entry point for packets from the networking stack, a regular chain may be used as jump target and is used for better rule organization.

**Note:** - IF - **Firewalld** is in use, this recommendation can be skipped.

##### **Rationale:**

If a base chain doesn't exist with a hook for input, forward, and delete, packets that would flow through those chains will not be touched by nftables.

##### **Impact:**

If configuring over ssh, **creating a base chain** with a policy of **drop** will cause loss of connectivity.

Ensure that a rule allowing ssh has been added to the base chain prior to setting the base chain's policy to drop

## Audit:

### - IF not using FirewallD -

Run the following command to verify that base chains exist for the **INPUT** filter hook:

```
# nft list ruleset | grep 'hook input'
```

Output should include:

```
type filter hook input
```

Run the following command to verify that base chains exist for the **FORWARD** filter hook:

```
# nft list ruleset | grep 'hook forward'
```

Output should include:

```
type filter hook forward
```

Run the following command to verify that base chains exist for the **OUTPUT** filter hook:

```
# nft list ruleset | grep 'hook output'
```

Output should include:

```
type filter hook output
```

**Note:** When using FirewallD the base chains are installed by default

## Remediation:

### - IF not using FirewallD -

Run the following command to create the base chains:

```
# nft create chain inet <table name> <base chain name> { type filter hook  
<(input|forward|output)> priority 0 \; }
```

*Example:*

```
# nft create chain inet filter input { type filter hook input priority 0 \; }  
# nft create chain inet filter forward { type filter hook forward priority 0  
\; }  
# nft create chain inet filter output { type filter hook output priority 0 \;  
}
```

## References:

1. NIST SP 800-53 Rev. 5: CA-9

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                           | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.4 <u>Implement and Manage a Firewall on Servers</u></b><br>Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.      |  |  |  |
| v7               | <b>9.4 <u>Apply Host-based Firewalls or Port Filtering</u></b><br>Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. |  |  |  |

#### *4.1.1.2 Ensure host based firewall loopback traffic is configured (Automated)*

**Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

**Description:**

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network

**Rationale:**

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

**Audit:**

Run the following script to verify that the loopback interface is configured:



```
#!/usr/bin/env bash

{
    l_output="" l_output2=""
    if nft list ruleset | awk '/hook\s+input\s+/,/\}\s*(#.*?)?$/ ' | grep -Pq --
'\H+\h+"lo"\h+accept'; then
        l_output="$l_output\n - Network traffic to the loopback address is
correctly set to accept"
    else
        l_output2="$l_output2\n - Network traffic to the loopback address is
not set to accept"
    fi
    l_ipsaddr="$(nft list ruleset | awk
'/filter_IN_public_deny|hook\s+input\s+/,/\}\s*(#.*?)?$/ ' | grep -P --
'ip\h+saddr') "
    if grep -Pq --
'ip\h+saddr\h+127\.0\.0\.0\/8\h+(counter\h+packets\h+\d+\h+bytes\h+\d+\h+)?dr
op' <<< "$l_ipsaddr" || grep -Pq --
'ip\h+daddr\h+!\!=\h+127\.0\.0\.1\h+ip\h+saddr\h+127\.0\.0\.1\h+drop' <<<
"$l_ipsaddr"; then
        l_output="$l_output\n - IPv4 network traffic from loopback address
correctly set to drop"
    else
        l_output2="$l_output2\n - IPv4 network traffic from loopback address
not set to drop"
    fi
    if grep -Pq -- '^h*0h*$' /sys/module/ipv6/parameters/disable; then
        l_ip6saddr="$(nft list ruleset | awk '/filter_IN_public_deny|hook
input/,/}/ ' | grep 'ip6 saddr') "
        if grep -Pq
'ip6\h+saddr\h+::1\h+(counter\h+packets\h+\d+\h+bytes\h+\d+\h+)?drop' <<<
"$l_ip6saddr" || grep -Pq --
'ip6\h+daddr\h+!\!=\h+::1\h+ip6\h+saddr\h+::1\h+drop' <<< "$l_ip6saddr"; then
            l_output="$l_output\n - IPv6 network traffic from loopback address
correctly set to drop"
        else
            l_output2="$l_output2\n - IPv6 network traffic from loopback address
not set to drop"
        fi
    fi
    if [ -z "$l_output2" ]; then
        echo -e "\n- Audit Result:\n  *** PASS ***\n$l_output"
    else
        echo -e "\n- Audit Result:\n  *** FAIL ***\n$l_output2\n\n - Correctly
set:\n$l_output"
    fi
}

```

## Remediation:

Run the following script to implement the loopback rules:

```

#!/usr/bin/env bash

{
    l_hbfw=""
    if systemctl is-enabled firewalld.service | grep -q 'enabled' && systemctl
is-enabled nftables.service | grep -q 'enabled'; then
        echo -e "\n - Error - Both FirewallD and Nftables are enabled\n -
Please follow recommendation: \"Ensure a single firewall configuration
utility is in use\""
        elif ! systemctl is-enabled firewalld.service | grep -q 'enabled' && !
systemctl is-enabled nftables.service | grep -q 'enabled'; then
            echo -e "\n - Error - Neither FirewallD or Nftables is enabled\n -
Please follow recommendation: \"Ensure a single firewall configuration
utility is in use\""
        else
            if systemctl is-enabled firewalld.service | grep -q 'enabled' && !
systemctl is-enabled nftables.service | grep -q 'enabled'; then
                echo -e "\n - FirewallD is in use on the system" && l_hbfw="fwd"
            elif ! systemctl is-enabled firewalld.service | grep -q 'enabled' &&
systemctl is-enabled nftables.service | grep -q 'enabled'; then
                echo -e "\n - Nftables is in use on the system" && l_hbfw="nft"
            fi
            l_ipsaddr="$(nft list ruleset | awk
'/filter_IN_public_deny|hook\s+input\s+/,/\}\s*(#.*?)?$/ ' | grep -P --
'ip\h+saddr')"
            if ! nft list ruleset | awk '/hook\s+input\s+/,/\}\s*(#.*?)?$/ ' | grep -
Pq -- '\H+\h+"lo"\h+accept'; then
                echo -e "\n - Enabling input to accept for loopback address"
                if [ "$l_hbfw" = "fwd" ]; then
                    firewall-cmd --permanent --zone=trusted --add-interface=lo
                    firewall-cmd --reload
                elif [ "$l_hbfw" = "nft" ]; then
                    nft add rule inet filter input iif lo accept
                fi
            fi
            if ! grep -Pq --
'ip\h+saddr\h+127\.0\.0\.0\/8\h+(counter\h+packets\h+\d+\h+bytes\h+\d+\h+)?dr
op' <<< "$l_ipsaddr" && ! grep -Pq --
'ip\h+daddr\h+!\h+=\h+127\.0\.0\.1\h+ip\h+saddr\h+127\.0\.0\.1\h+drop' <<<
"$l_ipsaddr"; then
                echo -e "\n - Setting IPv4 network traffic from loopback address to
drop"
                if [ "$l_hbfw" = "fwd" ]; then
                    firewall-cmd --permanent --add-rich-rule='rule family=ipv4 source
address="127.0.0.1" destination not address="127.0.0.1" drop'
                    firewall-cmd --permanent --zone=trusted --add-rich-rule='rule
family=ipv4 source address="127.0.0.1" destination not address="127.0.0.1"
drop'
                    firewall-cmd --reload
                elif [ "$l_hbfw" = "nft" ]; then
                    nft add rule inet filter input ip saddr 127.0.0.0/8 counter drop
                fi
            fi
            if grep -Pq -- '^h*0h*$' /sys/module/ipv6/parameters/disable; then
                l_ip6saddr="$(nft list ruleset | awk '/filter_IN_public_deny|hook
input/,/}/ ' | grep 'ip6 saddr')"
                if ! grep -Pq

```

```
'ip6\h+saddr\h+::1\h+(counter\h+packets\h+\d+\h+bytes\h+\d+\h+)?drop' <<<
"$l_ip6saddr" && ! grep -Pq --
'ip6\h+daddr\h+\!=\h+::1\h+ip6\h+saddr\h+::1\h+drop' <<< "$l_ip6saddr"; then
    echo -e "\n - Setting IPv6 network traffic from loopback address
to drop"
    if [ "$l_hbfbw" = "fwd" ]; then
        firewall-cmd --permanent --add-rich-rule='rule family=ipv6
source address="::1" destination not address="::1" drop'
        firewall-cmd --permanent --zone=trusted --add-rich-rule='rule
family=ipv6 source address="::1" destination not address="::1" drop'
        firewall-cmd --reload
    elif [ "$l_hbfbw" = "nft" ]; then
        nft add rule inet filter input ip6 saddr ::1 counter drop
    fi
fi
fi
fi
}
```

## References:

1. NIST SP 800-53 Rev. 5: CA-9

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                    | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.4 Implement and Manage a Firewall on Servers</b><br>Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.      |  |  |  |
| v7               | <b>9.4 Apply Host-based Firewalls or Port Filtering</b><br>Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.004            | TA0005  |             |

### 4.1.1.3 Ensure firewalld drops unnecessary services and ports (Manual)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

Services and ports can be accepted or explicitly rejected or dropped by a zone.

For every zone, you can set a default behavior that handles incoming traffic that is not further specified. Such behavior is defined by setting the target of the zone. There are three options - default, ACCEPT, REJECT, and DROP.

- ACCEPT - you accept all incoming packets except those disabled by a specific rule.
- REJECT - you disable all incoming packets except those that you have allowed in specific rules and the source machine is informed about the rejection.
- DROP - you disable all incoming packets except those that you have allowed in specific rules and no information sent to the source machine.

**Note:** - IF - **NFTables** is being used, this recommendation can be skipped.

#### Rationale:

To reduce the attack surface of a system, all services and ports should be blocked unless required

#### Audit:

Run the following command and review output to ensure that listed services and ports follow site policy.

```
# systemctl is-enabled firewalld.service | grep -q 'enabled' && firewall-cmd --list-all --zone="$(firewall-cmd --list-all | awk '/\ (active\)/ { print $1 }')" | grep -P -- '^h*(services:|ports:)'
```

## Remediation:

If Firewalld is in use on the system:

Run the following command to remove an unnecessary service:

```
# firewall-cmd --remove-service=<service>
```

*Example:*

```
# firewall-cmd --remove-service=cockpit
```

Run the following command to remove an unnecessary port:

```
# firewall-cmd --remove-port=<port-number>/<port-type>
```

*Example:*

```
# firewall-cmd --remove-port=25/tcp
```

Run the following command to make new settings persistent:

```
# firewall-cmd --runtime-to-permanent
```

## References:

1. firewalld.service(5)
2. NIST SP 800-53 Rev. 5: CA-9

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                    | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.4 Implement and Manage a Firewall on Servers</b><br>Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.      |  |  |  |
| v7               | <b>9.4 Apply Host-based Firewalls or Port Filtering</b><br>Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. |  |  |  |

#### 4.1.1.4 *Ensure nftables established connections are configured (Manual)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Configure the firewall rules for new outbound and established connections

##### **Rationale:**

If rules are not in place for established connections, all packets will be dropped by the default policy preventing network usage.

##### **Audit:**

If Nftables utility is in use on your system:

Run the following commands and verify all rules for established incoming connections match site policy:

```
# systemctl is-enabled nftables.service | grep -q 'enabled' && nft list ruleset | awk '/hook input/,/}/' | grep 'ct state'
```

Output should be similar to:

```
ip protocol tcp ct state established accept
ip protocol udp ct state established accept
ip protocol icmp ct state established accept
```

## Remediation:

If Nftables utility is in use on your system:

Configure nftables in accordance with site policy. The following commands will implement a policy to allow all established connections:

```
# systemctl is-enabled nftables.service | grep -q 'enabled' && nft add rule
inet filter input ip protocol tcp ct state established accept
# systemctl is-enabled nftables.service | grep -q 'enabled' && nft add rule
inet filter input ip protocol udp ct state established accept
# systemctl is-enabled nftables.service | grep -q 'enabled' && nft add rule
inet filter input ip protocol icmp ct state established accept
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                           | IG 1                                                                                 | IG 2                                                                                 | IG 3                                                                                 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| v8               | <b>4.4 <u>Implement and Manage a Firewall on Servers</u></b><br>Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.      |   |   |   |
| v7               | <b>9.4 <u>Apply Host-based Firewalls or Port Filtering</u></b><br>Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. |  |  |  |

### 4.1.1.5 Ensure nftables default deny firewall policy (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

Base chain policy is the default verdict that will be applied to packets reaching the end of the chain.

#### Rationale:

There are two policies: accept (Default) and drop. If the policy is set to **accept**, the firewall will accept any packet that is not configured to be denied and the packet will continue traversing the network stack.

It is easier to explicitly permit acceptable usage than to deny unacceptable usage.

**Note:** Changing firewall settings while connected over the network can result in being locked out of the system.

#### Impact:

If configuring nftables over ssh, creating a base chain with a policy of drop will cause loss of connectivity.

Ensure that a rule allowing **ssh** has been added to the base chain prior to setting the base chain's policy to drop

#### Audit:

If Nftables utility is in use on your system:

Run the following commands and verify that base chains contain a policy of **DROP**.

```
# systemctl --quiet is-enabled nftables.service && nft list ruleset | grep 'hook input' | grep -v 'policy drop'
```

Nothing should be returned

```
# systemctl --quiet is-enabled nftables.service && nft list ruleset | grep 'hook forward' | grep -v 'policy drop'
```

Nothing should be returned



## Remediation:

If NfTables utility is in use on your system:

Run the following command for the base chains with the input, forward, and output hooks to implement a default DROP policy:

```
# nft chain <table family> <table name> <chain name> { policy drop \; }
```

*Example:*

```
# nft chain inet filter input { policy drop \; }  
# nft chain inet filter forward { policy drop \; }
```

## Default Value:

accept

## References:

1. Manual Page nft
2. NIST SP 800-53 Rev. 5: CA-9

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                           | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.4 <u>Implement and Manage a Firewall on Servers</u></b><br>Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.      |  |  |  |
| v7               | <b>9.4 <u>Apply Host-based Firewalls or Port Filtering</u></b><br>Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. |  |  |  |

### *4.1.2 Ensure the firewall is configured to remove unnecessary use of functions, ports, protocols, and/or services (Manual)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the Ports, Protocols, and Services Management (PPSM) Category Assignments List (CAL) and vulnerability assessments.

#### **Rationale:**

To prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., VPN and IPS); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the operating system must support the organizational requirements, providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality-of-life issues.

**Audit:**

Inspect the firewall configuration and running services to verify it is configured to prohibit or restrict the use of functions, ports, protocols, and/or services that are unnecessary or prohibited.

Check which services are currently active with the following command:

```
# firewall-cmd --list-all-zones

custom (active)
target: DROP
icmp-block-inversion: no
interfaces: ens33
sources:
services: dhcpv6-client dns http https ldaps rpc-bind ssh
ports:
masquerade: no
forward-ports:
icmp-blocks:
rich rules:
```

Ask the System Administrator for the site or program Ports, Protocols, and Services Management Component Local Service Assessment (PPSM CLSA). Verify the services allowed by the firewall match the PPSM CLSA.

If there are additional ports, protocols, or services that are not in the PPSM CLSA, or there are ports, protocols, or services that are prohibited by the PPSM Category Assurance List (CAL), this is a finding.

**Remediation:**

Update the host's firewall settings and/or running services to comply with the PPSM Component Local Service Assessment (CLSA) for the site or program and the PPSM CAL.

**References:**

1. NIST SP 800-53 :: CM-7
2. NIST SP 800-53A :: CM-7.1 (iii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230500  
Rule ID: SV-230500r627750  
STIG ID: RHEL-08-040030  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                    | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.4 Implement and Manage a Firewall on Servers</b><br>Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.      |  |  |  |
| v7               | <b>9.4 Apply Host-based Firewalls or Port Filtering</b><br>Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. |  |  |  |

### 4.1.3 Ensure firewalld service is enabled and running (Automated)

#### Profile Applicability:

- STIG

#### Description:

Ensure that the firewalld service is enabled to protect your system

#### Rationale:

firewalld (Dynamic Firewall Manager) tool provides a dynamically managed firewall. The tool enables network/firewall zones to define the trust level of network connections and/or interfaces. It has support both for IPv4 and IPv6 firewall settings. Also, it supports Ethernet bridges and allow you to separate between runtime and permanent configuration options. Finally, it supports an interface for services or applications to add firewall rules directly

#### Impact:

Changing firewall settings while connected over network can result in being locked out of the system.

#### Audit:

Run the following command to verify that firewalld is enabled:

```
# systemctl is-enabled firewalld  
enabled
```

Run the following command to verify that firewalld is running

```
# firewall-cmd --state  
running
```

#### Remediation:

Run the following command to enable and start firewalld

```
# systemctl --now enable firewalld
```

#### References:

1. NIST SP 800-53 Revision 5 :: AC-17 (1)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244544  
Rule ID: SV-244544r854073  
STIG ID: RHEL-08-040101  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                    | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.4 Implement and Manage a Firewall on Servers</b><br>Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.      |  |  |  |
| v7               | <b>9.4 Apply Host-based Firewalls or Port Filtering</b><br>Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. |  |  |  |

## 4.1.4 Ensure nftables is installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

nftables provides a new in-kernel packet classification framework that is based on a network-specific Virtual Machine (VM) and a new nft userspace command line tool.

nftables reuses the existing Netfilter subsystems such as the existing hook infrastructure, the connection tracking system, NAT, userspace queuing and logging subsystem.

### Rationale:

nftables is a subsystem of the Linux kernel that can protect against threats originating from within a corporate network to include malicious mobile code and poorly configured software on a host.

### Impact:

Changing firewall settings while connected over the network can result in being locked out of the system.

### Audit:

Run the following command to verify that **nftables** is installed:

```
# rpm -q nftables  
nftables-<version>
```

### Remediation:

Run the following command to install **nftables**

```
# dnf install nftables
```

### References:

1. NIST SP 800-53 Rev. 5: CA-9

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                    | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.4 Implement and Manage a Firewall on Servers</b><br>Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.      |  |  |  |
| v7               | <b>9.4 Apply Host-based Firewalls or Port Filtering</b><br>Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations  |
|-----------------------------|---------|--------------|
| T1562, T1562.004            | TA0011  | M1031, M1037 |



### *4.1.5 Ensure a single firewall configuration utility is in use (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

In Linux security, employing a single, effective firewall configuration utility is crucial. Firewalls act as digital gatekeepers by filtering network traffic based on rules. Proper firewall configurations ensure that only legitimate traffic gets processed, reducing the system's exposure to potential threats. The choice between Firewalld and Nftables depends on organizational specific needs:

**Firewalld** - Is a firewall service daemon that provides a dynamic customizable host-based firewall with a D-Bus interface. Being dynamic, it enables creating, changing, and deleting the rules without the necessity to restart the firewall daemon each time the rules are changed.

**Nftables** - Includes the nft utility for configuration of the nftables subsystem of the Linux kernel.

#### **Notes:**

- firewalld with nftables backend does not support passing custom nftables rules to firewalld, using the **--direct** option.
- In order to configure firewall rules for nftables, a firewall utility needs to be installed and active of the system. The use of more than one firewall utility may produce unexpected results.

#### **Rationale:**

Proper configuration of a single firewall utility minimizes cyber threats and protects services and data, while avoiding vulnerabilities like open ports or exposed services. Standardizing on a single tool simplifies management, reduces errors, and fortifies security across Linux systems.

## Audit:

Run the following script to verify that a single firewall utility is in use on the system:

```
#!/usr/bin/env bash

{
    l_output="" l_output2="" l_fwd_status="" l_nft_status=""
    l_fwutil_status=""
    # Determine FirewallD utility Status
    rpm -q firewalld > /dev/null 2>&1 && l_fwd_status="$(systemctl is-enabled
firewalld.service):$(systemctl is-active firewalld.service)"
    # Determine NFTables utility Status
    rpm -q nftables > /dev/null 2>&1 && l_nft_status="$(systemctl is-enabled
nftables.service):$(systemctl is-active nftables.service)"
    l_fwutil_status="$l_fwd_status:$l_nft_status"
    case $l_fwutil_status in
        enabled:active:masked:inactive|enabled:active:disabled:inactive)
            l_output="\n - FirewallD utility is in use, enabled and active\n -
NFTables utility is correctly disabled or masked and inactive" ;;
        masked:inactive:enabled:active|disabled:inactive:enabled:active)
            l_output="\n - NFTables utility is in use, enabled and active\n -
FirewallD utility is correctly disabled or masked and inactive" ;;
        enabled:active:enabled:active)
            l_output2="\n - Both FirewallD and NFTables utilities are enabled
and active" ;;
        enabled:*:enabled:*)
            l_output2="\n - Both FirewallD and NFTables utilities are enabled"
;;
        *:active:*:active)
            l_output2="\n - Both FirewallD and NFTables utilities are enabled"
;;
        :enabled:active)
            l_output="\n - NFTables utility is in use, enabled, and active\n -
FirewallD package is not installed" ;;
        :)
            l_output2="\n - Neither FirewallD or NFTables is installed." ;;
        *:*:*)
            l_output2="\n - NFTables package is not installed on the system" ;;
        *)
            l_output2="\n - Unable to determine firewall state" ;;
    esac
    if [ -z "$l_output2" ]; then
        echo -e "\n- Audit Results:\n ** Pass **\n$l_output\n"
    else
        echo -e "\n- Audit Results:\n ** Fail **\n$l_output2\n"
    fi
}
```

## Remediation:

Run the following script to ensure that a single firewall utility is in use on the system:

```
#!/usr/bin/env bash

{
    l_output="" l_output2="" l_fwd_status="" l_nft_status=""
l_fwutil_status=""
    # Determine FirewallD utility Status
    rpm -q firewalld > /dev/null 2>&l1 && l_fwd_status="$(systemctl is-enabled
firewalld.service):$(systemctl is-active firewalld.service)"
    # Determine NFTables utility Status
    rpm -q nftables > /dev/null 2>&l1 && l_nft_status="$(systemctl is-enabled
nftables.service):$(systemctl is-active nftables.service)"
    l_fwutil_status="$l_fwd_status:$l_nft_status"
    case $l_fwutil_status in
        enabled:active:masked:inactive|enabled:active:disabled:inactive)
            echo -e "\n - FirewallD utility is in use, enabled and active\n -
NFTables utility is correctly disabled or masked and inactive\n - no
remediation required" ;;
        masked:inactive:enabled:active|disabled:inactive:enabled:active)
            echo -e "\n - NFTables utility is in use, enabled and active\n -
FirewallD utility is correctly disabled or masked and inactive\n - no
remediation required" ;;
        enabled:active:enabled:active)
            echo -e "\n - Both FirewallD and NFTables utilities are enabled and
active\n - stopping and masking NFTables utility"
            systemctl stop nftables && systemctl --now mask nftables ;;
        enabled:*:enabled:*)
            echo -e "\n - Both FirewallD and NFTables utilities are enabled\n -
remediating"
            if [ "$(awk -F: '{print $2}' <<< "$l_fwutil_status")" = "active" ]
&& [ "$(awk -F: '{print $4}' <<< "$l_fwutil_status")" = "inactive" ]; then
                echo " - masking NFTables utility"
                systemctl stop nftables && systemctl --now mask nftables
            elif [ "$(awk -F: '{print $4}' <<< "$l_fwutil_status")" = "active" ]
&& [ "$(awk -F: '{print $2}' <<< "$l_fwutil_status")" = "inactive" ]; then
                echo " - masking FirewallD utility"
                systemctl stop firewalld && systemctl --now mask firewalld
            fi ;;
        *:active:*:active)
            echo -e "\n - Both FirewallD and NFTables utilities are active\n -
remediating"
            if [ "$(awk -F: '{print $1}' <<< "$l_fwutil_status")" = "enabled" ]
&& [ "$(awk -F: '{print $3}' <<< "$l_fwutil_status")" != "enabled" ]; then
                echo " - stopping and masking NFTables utility"
                systemctl stop nftables && systemctl --now mask nftables
            elif [ "$(awk -F: '{print $3}' <<< "$l_fwutil_status")" = "enabled"
] && [ "$(awk -F: '{print $1}' <<< "$l_fwutil_status")" != "enabled" ]; then
                echo " - stopping and masking FirewallD utility"
                systemctl stop firewalld && systemctl --now mask firewalld
            fi ;;
        :enabled:active)
            echo -e "\n - NFTables utility is in use, enabled, and active\n -
FirewallD package is not installed\n - no remediation required" ;;
        :)
            echo -e "\n - Neither FirewallD or NFTables is installed.\n -
remediating\n - installing NFTables"
            dnf -q install nftables ;;
        *:*)
    
```

```

    echo -e "\n - Nftables package is not installed on the system\n -
remediating\n - installing Nftables"
    dnf -q install nftables ;;
*)
    echo -e "\n - Unable to determine firewall state" ;;
esac
}

```

## References:

1. [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/9/html-single/configuring\\_firewalls\\_and\\_packet\\_filters/index](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/configuring_firewalls_and_packet_filters/index)

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.4 Implement and Manage a Firewall on Servers</b><br>Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.                                 |    |    |    |
| v8               | <b>4.5 Implement and Manage a Firewall on End-User Devices</b><br>Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. |  |  |  |
| v7               | <b>9.4 Apply Host-based Firewalls or Port Filtering</b><br>Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.                            |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations  |
|-----------------------------|---------|--------------|
| T1562, T1562.004            | TA0011  | M1031, M1037 |

### 4.1.6 Ensure "nftables" is configured to allow rate limits on any connection to the system (Automated)

#### Profile Applicability:

- STIG

#### Description:

A firewall must be able to protect against or limit the effects of Denial of Service (DoS) attacks by ensuring the operating system can implement rate-limiting measures on impacted network interfaces.

#### Rationale:

DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of the operating system to mitigate the impact of DoS attacks that have occurred or are ongoing on system availability. For each system, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exists to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or establishing memory partitions). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

Since version 0.6.0, "firewalld" has incorporated "nftables" as its backend support. Utilizing the limit statement in "nftables" can help to mitigate DoS attacks.

#### Audit:

Verify "nftables" is configured to allow rate limits on any connection to the system with the following command:

Verify "firewalld" has "nftables" set as the default backend:

```
# grep -i firewallbackend /etc/firewalld/firewalld.conf  
  
# FirewallBackend  
FirewallBackend=nftables
```

If the "nftables" is not set as the "firewallbackend" default, this is a finding.

#### Remediation:

Configure "nftables" to be the default "firewallbackend" for "firewalld" by adding or editing the following line in "etc/firewalld/firewalld.conf":

```
FirewallBackend=nftables
```

Establish rate-limiting rules based on organization-defined types of DoS attacks on impacted network interfaces.

References:

- 1. NIST SP 800-53 Revision 5 :: SC-5 a

Additional Information:

|                                                                    |
|--------------------------------------------------------------------|
| Red Hat Enterprise Linux 8 Security Technical Implementation Guide |
| Version: 1 Release: 14 Benchmark Date: 24 Apr 2024                 |
| Vul ID: V-230525                                                   |
| Rule ID: SV-230525r902735                                          |
| STIG ID: RHEL-08-040150                                            |
| Severity: CAT II                                                   |

CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                    | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | 4.4 <u>Implement and Manage a Firewall on Servers</u><br>Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.      |    |    |    |
| v7               | 9.4 <u>Apply Host-based Firewalls or Port Filtering</u><br>Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. |  |  |  |

### 4.1.7 Ensure "firewalld" is installed (Automated)

#### Profile Applicability:

- STIG

#### Description:

A firewall must be installed on the operating system.

#### Rationale:

"Firewalld" provides an easy and effective way to block/limit remote access to the system via ports, services, and protocols.

Remote access services, such as those providing remote access to network devices and information systems, which lack automated control capabilities, increase risk and make remote user access management difficult at best.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

The operating system's functionality (e.g., RDP) must be capable of taking enforcement action if the audit reveals unauthorized activity. Automated control of remote access sessions allows organizations to ensure ongoing compliance with remote access policies by enforcing connection rules of remote access applications on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

#### Audit:

Verify that "firewalld" is installed with the following commands:

```
# dnf list installed firewalld
```

*Example output:*

```
firewalld.noarch 0.9.11-8.el8_10
```

If the "firewalld" package is not installed, ask the System Administrator if another firewall is installed. If no firewall is installed this is a finding.

#### Remediation:

Install "firewalld" with the following command:

```
# dnf install firewalld.noarch
```

#### References:

1. NIST SP 800-53 Revision 5 :: AC-17 (1)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230505  
Rule ID: SV-230505r854048  
STIG ID: RHEL-08-040100  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                    | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.4 Implement and Manage a Firewall on Servers</b><br>Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.      |  |  |  |
| v7               | <b>9.4 Apply Host-based Firewalls or Port Filtering</b><br>Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. |  |  |  |



#### *4.1.8 Ensure "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems (Manual)*

##### **Profile Applicability:**

- STIG

##### **Description:**

The firewall must employ a deny-all, allow-by-exception policy for allowing connections to other systems.

##### **Rationale:**

Failure to restrict network connectivity only to authorized systems permits inbound connections from malicious systems. It also permits outbound connections that may facilitate exfiltration of DoD data.

The operating system incorporates the "firewalld" daemon, which allows for many different configurations. One of these configurations is zones. Zones can be utilized to a deny-all, allow-by-exception approach. The default "drop" zone will drop all incoming network packets unless it is explicitly allowed by the configuration file or is related to an outgoing network connection.

##### **Audit:**

Verify "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems with the following commands:

```
# firewall-cmd --state
running
# firewall-cmd --get-active-zones

[custom]
interfaces: ens33
# firewall-cmd --info-zone=[custom] | grep target
target: DROP
```

If no zones are active on the operating system's interfaces or if the target is set to a different option other than "DROP", this is a finding.

## Remediation:

Configure the "firewalld" daemon to employ a deny-all, allow-by-exception with the following commands:

```
# firewall-cmd --permanent --new-zone=[custom]
# cp /usr/lib/firewalld/zones/drop.xml /etc/firewalld/zones/[custom].xml
```

This will provide a clean configuration file to work with that employs a deny-all approach. Next, add the exceptions that are required for mission functionality.  
**Note:** Add the exceptions that are required for mission functionality and update the short title in the xml file to match the [custom] zone name.

Reload the firewall rules to make the new [custom] zone available to load:

```
# firewall-cmd --reload
```

Set the default zone to the new [custom] zone:

```
# firewall-cmd --set-default-zone=[custom]
```

**Note:** This is a runtime and permanent change.

## References:

1. NIST SP 800-53 Revision 5 :: AC-17 (1)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230504  
Rule ID: SV-230504r942942  
STIG ID: RHEL-08-040090  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                    | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.4 Implement and Manage a Firewall on Servers</b><br>Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.      |  |  |  |
| v7               | <b>9.4 Apply Host-based Firewalls or Port Filtering</b><br>Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. |  |  |  |

## 5 Access Control

## 5.1 Configure SSH Server

Secure Shell (SSH) is a secure, encrypted replacement for common login services such as `telnet`, `ftp`, `rlogin`, `rsh`, and `rcp`. It is strongly recommended that sites abandon older clear-text login protocols and use SSH to prevent session hijacking and sniffing of sensitive data off the network.

The recommendations in this section only apply if the SSH daemon is installed on the system, **if remote access is not required the SSH daemon can be removed and this section skipped.**

`sshd_config`:

- The openSSH daemon configuration directives, `Include` and `Match`, may cause the audits in this section's recommendations to report incorrectly. It is recommended that these options only be used if they're needed and fully understood. If these options are configured in accordance with local site policy, they should be accounted for when following the recommendations in this section.
- The default `Include` location is the `/etc/ssh/sshd_config.d` directory. This default has been accounted for in this section. If a file has an additional `Include` that isn't this default location, the files should be reviewed to verify that the recommended setting is not being over-ridden.
- The audits of the running configuration in this section are run in the context of the root user, the local host name, and the local host's IP address. If a `Match` block exists that matches one of these criteria, the output of the audit will be from the match block. The respective matched criteria should be replaced with a non-matching substitution.
- **Include:**
  - Include the specified configuration file(s).
  - Multiple pathnames may be specified and each pathname may contain glob(7) wildcards that will be expanded and processed in lexical order.
  - Files without absolute paths are assumed to be in `/etc/ssh/`.
  - An Include directive may appear inside a Match block to perform conditional inclusion.

- **Match:**
  - Introduces a conditional block. If all of the criteria on the Match line are satisfied, the keywords on the following lines override those set in the global section of the config file, until either another Match line or the end of the file. If a keyword appears in multiple Match blocks that are satisfied, only the first instance of the keyword is applied.
  - The arguments to Match are one or more criteria-pattern pairs or the single token All which matches all criteria. The available criteria are User, Group, Host, LocalAddress, LocalPort, and Address.
  - The match patterns may consist of single entries or comma-separated lists and may use the wildcard and negation operators described in the PATTERNS section of ssh\_config(5).
  - The patterns in an Address criteria may additionally contain addresses to match in CIDR address/masklen format, such as 192.0.2.0/24 or 2001:db8::/32. Note that the mask length provided must be consistent with the address - it is an error to specify a mask length that is too long for the address or one with bits set in this host portion of the address. For example, 192.0.2.0/33 and 192.0.2.0/8, respectively.
  - Only a subset of keywords may be used on the lines following a Match keyword. Available keywords are available in the ssh\_config man page.
- Once all configuration changes have been made to /etc/ssh/sshd\_config or any included configuration files, the sshd configuration must be reloaded

Command to re-load the SSH daemon configuration:

```
# systemctl reload-or-restart sshd
```

sshd command:

- **-T** - Extended test mode. Check the validity of the configuration file, output the effective configuration to stdout and then exit. Optionally, Match rules may be applied by specifying the connection parameters using one or more **-C** options.
- **-C** - connection\_spec. Specify the connection parameters to use for the -T extended test mode. If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple **-C** options or as a comma-separated list. The keywords are addr, user, host, laddr, lport, and rdomain and correspond to source address, user, resolved source host name, local address, local port number and routing domain respectively.

### 5.1.1 Ensure openssh-server is installed (Automated)

#### Profile Applicability:

- STIG

#### Description:

All networked systems must have SSH installed.

#### Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

#### Audit:

Verify SSH is installed with the following command:

```
# dnf list installed openssh-server  
  
openssh-server.x86_64 8.0p1-5.el8 @anaconda
```

If the "SSH server" package is not installed, this is a finding.

#### Remediation:

Install SSH packages onto the host with the following command:

```
# dnf install openssh-server.x86_64
```

#### References:

1. NIST SP 800-53 Revision 5 :: SC-8

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244549  
Rule ID: SV-244549r916422  
STIG ID: RHEL-08-040159  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                         | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).                 |      |  |  |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                                |      |  |  |
| v7               | <b>16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u></b><br>Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels. |      |  |  |

### *5.1.2 Ensure permissions on /etc/ssh/sshd\_config are configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The file `/etc/ssh/sshd_config`, and files ending in `.conf` in the `/etc/ssh/sshd_config.d` directory, contain configuration specifications for `sshd`.

#### **Rationale:**

configuration specifications for `sshd` need to be protected from unauthorized changes by non-privileged users.



## Audit:

Run the following script and verify `/etc/ssh/sshd_config` and files ending in `.conf` in the `/etc/ssh/sshd_config.d` directory are:

- Mode `0600` or more restrictive
- Owned by the `root` user
- Group owned by the group `root`.

```
#!/usr/bin/env bash

{
  a_output=(); a_output2=()
  perm_mask='0177' && maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
  f_sshd_files_chk()
  {
    while IFS=: read -r l_mode l_user l_group; do
      a_out2=()
      [ "$l_mode & $perm_mask" ] -gt 0 ] && a_out2+=("    Is mode:
\"$l_mode\" \" \"
      "    should be mode: \"$maxperm\" or more restrictive")
      [ "$l_user" != "root" ] && a_out2+=("    Is owned by \"$l_user\"
should be owned by \"root\"")
      [ "$l_group" != "root" ] && a_out2+=("    Is group owned by
\"$l_user\" should be group owned by \"root\"")
      if [ "${#a_out2[@]}" -gt 0 ]; then
        a_output2+=(" - File: \"$l_file\": \" \" ${a_out2[@]}")
      else
        a_output+=(" - File: \"$l_file\": \" \"    Correct: mode ($l_mode),
owner ($l_user) \" \"
        "    and group owner ($l_group) configured")
      fi
      done <<(stat -Lc '%a:%U:%G' "$l_file")
    }
    [ -e "/etc/ssh/sshd_config" ] && l_file="/etc/ssh/sshd_config" &&
f_sshd_files_chk
    while IFS= read -r -d $'\0' l_file; do
      [ -e "$l_file" ] && f_sshd_files_chk
      done <<(find /etc/ssh/sshd_config.d -type f -name '*.conf' \( -perm /077
-o ! -user root -o ! -group root \) -print0 2>/dev/null)
      if [ "${#a_output2[@]}" -le 0 ]; then
        printf '%s\n' "" "- Audit Result: \" \"    ** PASS ** \" \" ${a_output[@]} \" \"
      else
        printf '%s\n' "" "- Audit Result: \" \"    ** FAIL ** \" \" - Reason(s) for
audit failure: \" \" ${a_output2[@]} \" \"
        [ "${#a_output2[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set: \"
\" ${a_output[@]} \" \"
      fi
    }
  }
}
```

- IF - other locations are listed in an `Include` statement, `*.conf` files in these locations should also be checked.

## Remediation:

Run the following script to set ownership and permissions on `/etc/ssh/sshd_config` and files ending in `.conf` in the `/etc/ssh/sshd_config.d` directory:

```
#!/usr/bin/env bash

{
  chmod u-x,og-rwx /etc/ssh/sshd_config
  chown root:root /etc/ssh/sshd_config
  while IFS= read -r -d $'\0' l_file; do
    if [ -e "$l_file" ]; then
      chmod u-x,og-rwx "$l_file"
      chown root:root "$l_file"
    fi
  done < <(find /etc/ssh/sshd_config.d -type f -print0 2>/dev/null)
}
```

- IF - other locations are listed in an **Include** statement, `*.conf` files in these locations access should also be modified.

## References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1098, T1098.004, T1543, T1543.002 | TA0005  | M1022       |

### *5.1.3 Ensure permissions on SSH private host key files are configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### **Description:**

An SSH private key is one of two files used in SSH public key authentication. In this authentication method, the possession of the private key is proof of identity. Only a private key that corresponds to a public key will be able to authenticate successfully. The private keys need to be stored and handled carefully, and no copies of the private key should be distributed.

#### **Rationale:**

If an unauthorized user obtains the private SSH host key file, the host could be impersonated

#### **Audit:**

Run the following script to verify SSH private host key files are owned by the root user and either:

- owned by the group root and mode **0600** or more restrictive

#### **- OR -**

- owned by the group designated to own openSSH private keys and mode **0640** or more restrictive

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=()
    l_ssh_group_name="$(awk -F: '($1 ~ /^(ssh_keys|_?ssh)$/) {print $1}'
/etc/group)"
    f_file_chk()
    {
        while IFS=: read -r l_file_mode l_file_owner l_file_group; do
            a_out2=()
            [ "$l_file_group" = "$l_ssh_group_name" ] && l_pmask="0137" ||
l_pmask="0177"
            l_maxperm="$( printf '%o' $(( 0777 & ~$l_pmask )) )"
            if [ $(( $l_file_mode & $l_pmask )) -gt 0 ]; then
                a_out2+=("    Mode: \"$l_file_mode\" should be mode:
\"$l_maxperm\" or more restrictive")
            fi
            if [ "$l_file_owner" != "root" ]; then
                a_out2+=("    Owned by: \"$l_file_owner\" should be owned by
\"root\"")
            fi
            if [[ ! "$l_file_group" =~ ($l_ssh_group_name|root) ]]; then
                a_out2+=("    Owned by group \"$l_file_group\" should be group
owned by: \"$l_ssh_group_name\" or \"root\"")
            fi
            if [ "${#a_out2[@]}" -gt 0 ]; then
                a_output2+=(" - File: \"$l_file\"${a_out2[@]}")
            else
                a_output+=(" - File: \"$l_file\" \" \" \
                \"    Correct: mode: \"$l_file_mode\", owner: \"$l_file_owner\"
and group owner: \"$l_file_group\" configured")
            fi
            done < <(stat -Lc '%a:%U:%G' "$l_file")
        }
        while IFS= read -r -d $'\0' l_file; do
            if ssh-keygen -lf &>/dev/null "$l_file"; then
                file "$l_file" | grep -Piq --
'\bopenssh\b+([\#\n\r]+\b)?private\b+key\b' && f_file_chk
            fi
            done < <(find -L /etc/ssh -xdev -type f -print0 2>/dev/null)
            if [ "${#a_output2[@]}" -le 0 ]; then
                printf '%s\n' "" "- Audit Result:" "    ** PASS **" "${a_output[@]}" ""
            else
                printf '%s\n' "" "- Audit Result:" "    ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
                [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:"
"${a_output[@]}" ""
            fi
        }
    }
}

```

## Remediation:

Run the following script to set mode, ownership, and group on the private SSH host key files:

```
#!/usr/bin/env bash

{
  a_output=(); a_output2=(); l_ssh_group_name="$(awk -F: '($1 ~ /^(ssh_keys|_?ssh)$/) {print $1}' /etc/group)"
  f_file_access_fix()
  {
    while IFS=: read -r l_file_mode l_file_owner l_file_group; do
      a_out2=()
      [ "$l_file_group" = "$l_ssh_group_name" ] && l_pmask="0137" || l_pmask="0177"
      l_maxperm="$( printf '%o' $(( 0777 & ~$l_pmask )) )"
      if [ $(( $l_file_mode & $l_pmask )) -gt 0 ]; then
        a_out2+=("      Mode: \"$l_file_mode\" should be mode: \"$l_maxperm\" or more restrictive" \
          "      updating to mode: \"$l_maxperm\"")
        if [ "l_file_group" = "$l_ssh_group_name" ]; then
          chmod u-x,g-wx,o-rwx "$l_file"
        else
          chmod u-x,go-rwx "$l_file"
        fi
      fi
      if [ "$l_file_owner" != "root" ]; then
        a_out2+=("      Owned by: \"$l_file_owner\" should be owned by \"root\"" \
          "      Changing ownership to \"root\"")
        chown root "$l_file"
      fi
      if [[ ! "$l_file_group" =~ ($l_ssh_group_name|root) ]]; then
        [ -n "$l_ssh_group_name" ] && l_new_group="$l_ssh_group_name" || l_new_group="root"
        a_out2+=("      Owned by group \"$l_file_group\" should be group owned by: \"$l_ssh_group_name\" or \"root\"" \
          "      Changing group ownership to \"$l_new_group\"")
        chgrp "$l_new_group" "$l_file"
      fi
      if [ "${#a_out2[@]}" -gt "0" ]; then
        a_output2+=(" - File: \"$l_file\" \"${a_out2[@]}")
      else
        a_output+=(" - File: \"$l_file\" \
          "Correct: mode: \"$l_file_mode\", owner: \"$l_file_owner\", and group owner: \"$l_file_group\" configured")
      fi
      done < <(stat -Lc '%#a:%U:%G' "$l_file")
    }
    while IFS= read -r -d $'\0' l_file; do
      if ssh-keygen -lf &>/dev/null "$l_file"; then
        file "$l_file" | grep -Piq -- '\bopenssh\b+([^\n\r]+\h+)?private\b+h+key\b' &&
        f_file_access_fix
      fi
      done < <(find -L /etc/ssh -xdev -type f -print0 2>/dev/null)
      if [ "${#a_output2[@]}" -le "0" ]; then
        printf '%s\n' "" " - No access changes required" ""
      else
        printf '%s\n' "" " - Remediation results:" "${a_output2[@]}" ""
      fi
    fi
  }
}
```

## References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230287  
Rule ID: SV-230287r880714  
STIG ID: RHEL-08-010490  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics        | Mitigations |
|-----------------------------|----------------|-------------|
| T1552, T1552.004            | TA0003, TA0006 | M1022       |

### *5.1.4 Ensure permissions on SSH public host key files are configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### **Description:**

An SSH public key is one of two files used in SSH public key authentication. In this authentication method, a public key is a key that can be used for verifying digital signatures generated using a corresponding private key. Only a public key that corresponds to a private key will be able to authenticate successfully.

#### **Rationale:**

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

#### **Audit:**

Run the following command and verify Access does not grant write or execute permissions to group or other for all returned files:

Run the following script to verify SSH public host key files are mode **0644** or more restrictive, owned by the **root** user, and owned by the **root** group:

```

#!/usr/bin/env bash

{
    a_output=(); a_output2=()
    l_pmask="0133"; l_maxperm="$( printf '%o' $(( 0777 & ~$l_pmask )) )"
    f_file_chk()
    {
        while IFS= read -r l_file_mode l_file_owner l_file_group; do
            a_out2=()
            if [ $(( $l_file_mode & $l_pmask )) -gt 0 ]; then
                a_out2+=("    Mode: \"$l_file_mode\" should be mode:
\"$l_maxperm\" or more restrictive")
            fi
            if [ "$l_file_owner" != "root" ]; then
                a_out2+=("    Owned by: \"$l_file_owner\" should be owned by:
\"root\"")
            fi
            if [ "$l_file_group" != "root" ]; then
                a_out2+=("    Owned by group \"$l_file_group\" should be group
owned by group: \"root\"")
            fi
            if [ "${#a_out2[@]}" -gt 0 ]; then
                a_output2+=(" - File: \"$l_file\" \"${a_out2[@]}")
            else
                a_output+=(" - File: \"$l_file\" \
                "    Correct: mode: \"$l_file_mode\", owner: \"$l_file_owner\"
and group owner: \"$l_file_group\" configured")
            fi
            done < <(stat -Lc '%a:%U:%G' "$l_file")
        }
        while IFS= read -r -d $'\0' l_file; do
            if ssh-keygen -lf &>/dev/null "$l_file"; then
                file "$l_file" | grep -Piq --
'\bopenssh\h+([\#\n\r]+\h+)?public\h+key\b' && f_file_chk
            fi
            done < <(find -L /etc/ssh -xdev -type f -print0 2>/dev/null)
            if [ "${#a_output2[@]}" -le 0 ]; then
                [ "${#a_output[@]}" -le 0 ] && a_output+=(" - No openSSH public keys
found")
                printf '%s\n' "" "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
            else
                printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
                [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "" "- Correctly set:"
"${a_output[@]}" ""
            fi
        }
    }
}

```



## Remediation:

Run the following script to set mode, ownership, and group on the public SSH host key files:

```
#!/usr/bin/env bash

{
  a_output=(); a_output2=()
  l_pmask="0133"; l_maxperm="$( printf '%o' $(( 0777 & ~$l_pmask )) )"
  f_file_access_fix()
  {
    while IFS=: read -r l_file_mode l_file_owner l_file_group; do
      a_out2=()
      [ $(( $l_file_mode & $l_pmask )) -gt 0 ] && \
        a_out2+=("      Mode: \"$l_file_mode\" should be mode: \
\"$l_maxperm\" or more restrictive" \
        "      updating to mode: \"$l_maxperm\"") && chmod u-x,go-wx
      "$l_file"
      [ "$l_file_owner" != "root" ] && \
        a_out2+=("      Owned by: \"$l_file_owner\" should be owned by \
\"root\"" \
        "      Changing ownership to \"root\"") && chown root "$l_file"
      [ "$l_file_group" != "root" ] && \
        a_out2+=("      Owned by group \"$l_file_group\" should be group \
owned by: \"root\"" \
        "      Changing group ownership to \"root\"") && chgrp root
      "$l_file"
      if [ "${#a_out2[@]}" -gt 0 ]; then
        a_output2+=(" - File: \"$l_file\" \"${a_out2[@]}")
      else
        a_output+=(" - File: \"$l_file\" \
        "      Correct: mode: \"$l_file_mode\", owner: \"$l_file_owner\", \
and group owner: \"$l_file_group\" configured")
      fi
      done < <(stat -Lc '%a:%U:%G' "$l_file")
    }
    while IFS= read -r -d $'\0' l_file; do
      if ssh-keygen -lf &>/dev/null "$l_file"; then
        file "$l_file" | grep -Piq --
'\bopenssh\h+([\^#\n\r]+\h+)?public\h+key\b' && f_file_access_fix
      fi
      done < <(find -L /etc/ssh -xdev -type f -print0 2>/dev/null)
      if [ "${#a_output2[@]}" -le 0 ]; then
        printf '%s\n' "" " - No access changes required" ""
      else
        printf '%s\n' " - Remediation results:" "${a_output2[@]}" ""
      fi
    fi
  }
}
```

## Default Value:

644 0/root 0/root

## References:

1. NIST SP 800-53 Rev. 5: AC-3 CM-6 b MP-2
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230286  
Rule ID: SV-230286r627750  
STIG ID: RHEL-08-010480  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |    |    |    |
| v7               | <b>14.6 Protect Information through Access Control Lists</b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics        | Mitigations |
|-----------------------------|----------------|-------------|
| T1557, T1557.000            | TA0003, TA0006 | M1022       |

### 5.1.5 Ensure sshd access is configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged:

- **AllowUsers:**
  - The **AllowUsers** variable gives the system administrator the option of allowing specific users to **ssh** into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of user@host.
- **AllowGroups:**
  - The **AllowGroups** variable gives the system administrator the option of allowing specific groups of users to **ssh** into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.
- **DenyUsers:**
  - The **DenyUsers** variable gives the system administrator the option of denying specific users to **ssh** into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of user@host.
- **DenyGroups:**
  - The **DenyGroups** variable gives the system administrator the option of denying specific groups of users to **ssh** into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.

#### Rationale:

Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

## Audit:

Run the following command and verify the output:

```
# sshd -T | grep -Pi -- '^h*(allow|deny) (users|groups) \h+\H+'
```

Verify that the output matches at least one of the following lines:

```
allowusers <userlist>
-OR-
allowgroups <grouplist>
-OR-
denyusers <userlist>
-OR-
denygroups <grouplist>
```

Review the list(s) to ensure included users and/or groups follow local site policy  
- **IF - Match** set statements are used in your environment, specify the connection parameters to use for the **-T** extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user **sshuser**:*

```
# sshd -T -C user=sshuser | grep -Pi --
'^h*(allow|deny) (users|groups) \h+\H+'
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple **-C** options or as a comma-separated list. The keywords are **addr** (source address), **user** (user), **host** (resolved source host name), **laddr** (local address), **lport** (local port number), and **rdomain** (routing domain).

## Remediation:

Edit the `/etc/ssh/sshd_config` file to set one or more of the parameters above any **Include** and **Match** set statements as follows:

```
AllowUsers <userlist>
- AND/OR -
AllowGroups <grouplist>
```

## Note:

- First occurrence of a option takes precedence, **Match** set statements withstanding. If **Include** locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a **.conf** file in a **Include** directory.
- **Be advised** that these options are "ANDed" together. If both **AllowUsers** and **AllowGroups** are set, connections will be limited to the list of users that are also a member of an allowed group. It is recommended that only one be set for clarity and ease of administration.
- It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user or group and forget to add it to the deny list.

## Default Value:

None

## References:

1. SSHD\_CONFIG(5)
2. NIST SP 800-53 Rev. 5: AC-3. MP-2
3. SSHD(8)

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                 | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                          |  |  |  |
| v7               | <b>4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u></b><br>Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities. |  |  |  |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1021, T1021.004                   | TA0008         | M1018              |

### *5.1.6 Ensure sshd Banner is configured (Automated)*

**Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

**Description:**

The **Banner** parameter specifies a file whose contents must be sent to the remote user before authentication is permitted. By default, no banner is displayed.

**Rationale:**

Banners are used to warn connecting users of the particular site's policy regarding connection. Presenting a warning message prior to the normal user login may assist the prosecution of trespassers on the computer system.

## Audit:

Run the following command to verify **Banner** is set:

```
# sshd -T | grep -Pi -- '^banner\h+\//\H+'
```

*Example:*

```
banner /etc/issue.net
```

- **IF - Match** set statements are used in your environment, specify the connection parameters to use for the **-T** extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user **sshuser**:*

```
# sshd -T -C user=sshuser | grep -Pi -- '^banner\h+\//\H+'
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple **-C** options or as a comma-separated list. The keywords are **addr** (source address), **user** (user), **host** (resolved source host name), **laddr** (local address), **lport** (local port number), and **rdomain** (routing domain).

Run the following command and verify that the contents or the file being called by the **Banner** argument match site policy:

```
# [ -e "$(sshd -T | awk '$1 == "banner" {print $2}')" ] && cat "$(sshd -T | awk '$1 == "banner" {print $2}')"
```

Run the following command and verify no results are returned:

```
# grep -Psi -- "(\v|r|m|s\b$(grep '^ID=' /etc/os-release | cut -d= -f2 | sed -e 's/"/g')\b)" "$(sshd -T | awk '$1 == "banner" {print $2}')"
```



## Remediation:

Edit the `/etc/ssh/sshd_config` file to set the **Banner** parameter above any **Include** and **Match** entries as follows:

```
Banner /etc/issue.net
```

**Note:** First occurrence of a option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location. Edit the file being called by the **Banner** argument with the appropriate contents according to your site policy, remove any instances of `\m`, `\r`, `\s`, `\v` or references to the **OS platform**

*Example:*

```
# printf '%s\n' "Authorized users only. All activity may be monitored and  
reported." > "$(sshd -T | awk '$1 == "banner" {print $2}')
```

## References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics        | Mitigations |
|-----------------------------|----------------|-------------|
|                             | TA0001, TA0007 | M1035       |

### 5.1.7 Ensure sshd Ciphers are configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

This variable limits the ciphers that SSH can use during communication.

#### Notes:

- Some organizations may have stricter requirements for approved ciphers.
- Ensure that ciphers used are in compliance with site policy.
- The only "strong" ciphers currently FIPS 140 compliant are:
  - [aes256-gcm@openssh.com](#)
  - [aes128-gcm@openssh.com](#)
  - aes256-ctr
  - aes192-ctr
  - aes128-ctr

#### Rationale:

Weak ciphers that are used for authentication to the cryptographic module cannot be relied upon to provide confidentiality or integrity, and system data may be compromised.

- The Triple DES ciphers, as used in SSH, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain clear text data via a birthday attack against a long-duration encrypted session, aka a "Sweet32" attack.
- Error handling in the SSH protocol; Client and Server, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plain text data from an arbitrary block of cipher text in an SSH session via unknown vectors.

## Audit:

Run the following command to verify none of the "weak" ciphers are being used:

```
# sshd -T | grep -Pi --
'^ciphers\h+\\"?([^\n\r]+),)?((3des|blowfish|cast128|aes(128|192|256))-
cbc|arcfour(128|256)?|rijndael-cbc@lysator\.liu\.se|chacha20-
poly1305@openssh\.com)\b'
```

- **IF** - a line is returned, review the list of ciphers. If the line includes **chacha20-poly1305@openssh.com**, review **CVE-2023-48795** and verify the system has been patched. No ciphers in the list below should be returned as they're considered "weak":

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
```

## Remediation:

### Note:

- First occurrence of an option takes precedence.
- Though ciphers may be configured through the **Ciphers** option in the **/etc/ssh/sshd\_config** file, it is recommended that the ciphers available to openSSH server are configured through system-wide-crypto-policy
- If the recommendations in the subsection "Configure system wide crypto policy" have been followed, this Audit should be in a passing state. Please review that section before following this Remediation Procedure
- By default, system-wide-crypto-policy is applied to the openSSH server. If the following defaults don't exist due to modifications or upgrade from a earlier release, the system-wide-crypto-policy may not be included by the openSSH server. It is recommended that these defaults be restored, created, or the line **Include /etc/crypto-policies/back-ends/opensshserver.config** be added before any lines containing the **Cipher** argument.
- Defaults:
  - The file **/etc/ssh/sshd\_config** includes the line: **Include /etc/ssh/sshd\_config.d/\*.conf**. This line must appear before any lines containing the **Cipher** argument
  - This directory **/etc/ssh/sshd\_config.d/** includes a file **/etc/ssh/sshd\_config.d/50-redhat.conf**
  - The file **/etc/ssh/sshd\_config.d/50-redhat.conf** includes the line **Include /etc/crypto-policies/back-ends/opensshserver.config**
  - The file **/etc/crypto-policies/back-ends/opensshserver.config** is generated by system-wide-crypto-policy

- **IF** - **CVE-2023-48795** has been addressed, and it meets local site policy, **chacha20-poly1305** may be removed from the list of excluded ciphers.

Create or edit a file in **/etc/crypto-policies/policies/modules/** ending in **.pmod** and add or modify the the following line:

```
cipher@SSH = -3DES-CBC -AES-128-CBC -AES-192-CBC -AES-256-CBC -CHACHA20-POLY1305
```

*Example:*

```
# printf '%s\n' "# This is a subpolicy to disable weak ciphers" "# for the  
SSH protocol (libssh and OpenSSH)" "cipher@SSH = -3DES-CBC -AES-128-CBC -AES-  
192-CBC -AES-256-CBC -CHACHA20-POLY1305" >> /etc/crypto-  
policies/policies/modules/NO-SSHWEAKCIPHERS.pmod
```

Run the following command to update the system-wide cryptographic policy

```
# update-crypto-policies --set  
<CRYPTO_POLICY>:<CRYPTO_SUBPOLICY1>:<CRYPTO_SUBPOLICY2>:<CRYPTO_SUBPOLICY3>
```

*Example:*

```
# update-crypto-policies --set DEFAULT:NO-SHA1:NO-WEAKMAC:NO-SSHCBC:NO-  
SSHCHACHA20:NO-SSHWEAKCIPHERS
```

Run the following command to reload the openSSH server to make your cryptographic settings effective:

```
# systemctl reload-or-restart sshd
```

- **OR** - If system-wide-crypto-policy is not being used to configure available ciphers (**This is not recommended**)

Edit the **/etc/ssh/sshd\_config** file and add/modify the **Ciphers** line to contain a comma separated list of the site unapproved (weak) Ciphers preceded with a **-** above any **Include** entries:

*Example:*

```
Ciphers -3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,chacha20-  
poly1305@openssh.com
```

**Default Value:**

Ciphers [chacha20-poly1305@openssh.com](#),aes128-ctr,aes192-ctr,aes256-ctr,[aes128-gcm@openssh.com](#),[aes256-gcm@openssh.com](#)

**References:**

1. <https://nvd.nist.gov/vuln/detail/CVE-2023-48795>
2. <https://nvd.nist.gov/vuln/detail/CVE-2019-1543>
3. <https://nvd.nist.gov/vuln/detail/CVE-2016-2183>
4. <https://nvd.nist.gov/vuln/detail/CVE-2008-5161>
5. <https://www.openssh.com/txt/cbc.adv>
6. <https://www.openssh.com/txt/cbc.adv>
7. SSHD\_CONFIG(5)
8. NIST SP 800-53 Rev. 5: SC-8

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                  | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | 3.10 <u>Encrypt Sensitive Data in Transit</u><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |      | ●    | ●    |
| v7               | 14.4 <u>Encrypt All Sensitive Information in Transit</u><br>Encrypt all sensitive information in transit.                                                                                |      | ●    | ●    |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1040, T1040.000, T1557     | TA0006  | M1041       |

### 5.1.8 Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

**Note:** To clarify, the two settings described below are only meant for idle connections from a protocol perspective and are not meant to check if the user is active or not. An idle user does not mean an idle connection. SSH does not and never had, intentionally, the capability to drop idle users. In SSH versions before 8.2p1 there was a bug that caused these values to behave in such a manner that they were abused to disconnect idle users. This bug has been resolved in 8.2p1 and thus it can no longer be abused to disconnect idle users.

The two options `ClientAliveInterval` and `ClientAliveCountMax` control the timeout of SSH sessions. Taken directly from `man 5 sshd_config`:

- `ClientAliveInterval` Sets a timeout interval in seconds after which if no data has been received from the client, sshd(8) will send a message through the encrypted channel to request a response from the client. The default is 0, indicating that these messages will not be sent to the client.
- `ClientAliveCountMax` Sets the number of client alive messages which may be sent without sshd(8) receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, sshd will disconnect the client, terminating the session. It is important to note that the use of client alive messages is very different from TCPKeepAlive. The client alive messages are sent through the encrypted channel and therefore will not be spoofable. The TCP keepalive option enabled by TCPKeepAlive is spoofable. The client alive mechanism is valuable when the client or server depend on knowing when a connection has become unresponsive. The default value is 3. If `ClientAliveInterval` is set to 15, and `ClientAliveCountMax` is left at the default, unresponsive SSH clients will be disconnected after approximately 45 seconds. Setting a zero `ClientAliveCountMax` disables connection termination.

## Rationale:

In order to prevent resource exhaustion, appropriate values should be set for both `ClientAliveInterval` and `ClientAliveCountMax`. Specifically, looking at the source code, `ClientAliveCountMax` must be greater than zero in order to utilize the ability of SSH to drop idle connections. If connections are allowed to stay open indefinitely, this can potentially be used as a DDOS attack or simple resource exhaustion could occur over unreliable networks.

The example set here is a 45 second timeout. Consult your site policy for network timeouts and apply as appropriate.

## Audit:

Run the following command and verify `ClientAliveInterval` and `ClientAliveCountMax` are greater than zero:

```
# sshd -T | grep -Pi -- '(clientaliveinterval|clientalivecountmax)'
```

*Example Output:*

```
clientaliveinterval 15
clientalivecountmax 3
```

- IF - **Match** set statements are used in your environment, specify the connection parameters to use for the `-T` extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user `sshuser`:*

```
# sshd -T -C user=sshuser | grep -Pi --
'(clientaliveinterval|clientalivecountmax)'
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple `-C` options or as a comma-separated list. The keywords are `addr` (source address), `user` (user), `host` (resolved source host name), `laddr` (local address), `lport` (local port number), and `rdomain` (routing domain).

## Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `ClientAliveInterval` and `ClientAliveCountMax` parameters above any **Include** and **Match** entries according to site policy.

*Example:*

```
ClientAliveInterval 15
ClientAliveCountMax 3
```

**Note:** First occurrence of an option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

**Default Value:**

ClientAliveInterval 0

ClientAliveCountMax 3

**References:**

1. SSHD\_CONFIG(5)
2. SSHD(8)
3. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

**Additional Information:**

[https://bugzilla.redhat.com/show\\_bug.cgi?id=1873547](https://bugzilla.redhat.com/show_bug.cgi?id=1873547)

[https://github.com/openssh/openssh-portable/blob/V\\_8\\_9/serverloop.c#L137](https://github.com/openssh/openssh-portable/blob/V_8_9/serverloop.c#L137)

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques            | Tactics | Mitigations |
|----------------------------------------|---------|-------------|
| T1078, T1078.001, T1078.002, T1078.003 | TA0001  | M1026       |



## 5.1.9 Ensure sshd DisableForwarding is enabled (Automated)

### Profile Applicability:

- Level 1 - Workstation
- Level 2 - Server

### Description:

The **DisableForwarding** parameter disables all forwarding features, including X11, ssh-agent(1), TCP and StreamLocal. This option overrides all other forwarding-related options and may simplify restricted configurations.

- X11Forwarding provides the ability to tunnel X11 traffic through the connection to enable remote graphic connections.
- ssh-agent is a program to hold private keys used for public key authentication. Through use of environment variables the agent can be located and automatically used for authentication when logging in to other machines using ssh.
- SSH port forwarding is a mechanism in SSH for tunneling application ports from the client to the server, or servers to clients. It can be used for adding encryption to legacy applications, going through firewalls, and some system administrators and IT professionals use it for opening backdoors into the internal network from their home machines.

### Rationale:

Disable X11 forwarding unless there is an operational requirement to use X11 applications directly. There is a small risk that the remote X11 servers of users who are logged in via SSH with X11 forwarding could be compromised by other users on the X11 server. Note that even if X11 forwarding is disabled, users can always install their own forwarders.

anyone with root privilege on the the intermediate server can make free use of ssh-agent to authenticate them to other servers

Leaving port forwarding enabled can expose the organization to security risks and backdoors. SSH connections are protected with strong encryption. This makes their contents invisible to most deployed network monitoring and traffic filtering solutions. This invisibility carries considerable risk potential if it is used for malicious purposes such as data exfiltration. Cybercriminals or malware could exploit SSH to hide their unauthorized communications, or to exfiltrate stolen data from the target network.

## Impact:

SSH tunnels are widely used in many corporate environments. In some environments the applications themselves may have very limited native support for security. By utilizing tunneling, compliance with SOX, HIPAA, PCI-DSS, and other standards can be achieved without having to modify the applications.

## Audit:

Run the following command to verify **DisableForwarding** is set to **yes**:

```
# sshd -T | grep -i disableforwarding  
disableforwarding yes
```

## Remediation:

Edit the **/etc/ssh/sshd\_config** file to set the **DisableForwarding** parameter to **yes** above any **Include** entry as follows:

```
DisableForwarding yes
```

**Note:** First occurrence of a option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

## References:

1. sshd\_config(5)
2. SSHD(8)
3. NIST SP 800-53 Rev. 5: CM-7

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1210, T1210.000                   | TA0008         | M1042              |

### 5.1.10 Ensure sshd GSSAPIAuthentication is disabled (Automated)

#### Profile Applicability:

- Level 1 - Workstation
- Level 2 - Server
- STIG

#### Description:

The **GSSAPIAuthentication** parameter specifies whether user authentication based on GSSAPI is allowed

#### Rationale:

Allowing GSSAPI authentication through SSH exposes the system's GSSAPI to remote hosts, and should be disabled to reduce the attack surface of the system

#### Audit:

Run the following command to verify **GSSAPIAuthentication** is set to **no**:

```
# sshd -T | grep gssapiauthentication  
gssapiauthentication no
```

- **IF - Match** set statements are used in your environment, specify the connection parameters to use for the **-T** extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user **sshuser**:*

```
# sshd -T -C user=sshuser | grep gssapiauthentication
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple **-C** options or as a comma-separated list. The keywords are **addr** (source address), **user** (user), **host** (resolved source host name), **laddr** (local address), **lport** (local port number), and **rdomain** (routing domain)

## Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `GSSAPIAuthentication` parameter to `no` above any `Include` and `Match` entries as follows:

```
GSSAPIAuthentication no
```

**Note:** First occurrence of an option takes precedence, `Match` set statements withstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

## Default Value:

GSSAPIAuthentication no

## References:

1. SSHD\_CONFIG(5)
2. SSHD(8)
3. NIST SP 800-53 :: CM-6 b
4. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-244528  
Rule ID: SV-244528r952106  
STIG ID: RHEL-08-010522  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                       |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1078, T1078.001, T1078.003 | TA0001  | M1042       |

### 5.1.11 Ensure sshd HostbasedAuthentication is disabled (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The **HostbasedAuthentication** parameter specifies if authentication is allowed through trusted hosts via the user of **.rhosts**, or **/etc/hosts.equiv**, along with successful public key client host authentication.

#### Rationale:

Even though the **.rhosts** files are ineffective if support is disabled in **/etc/pam.conf**, disabling the ability to use **.rhosts** files in SSH provides an additional layer of protection.

#### Audit:

Run the following command to verify **HostbasedAuthentication** is set to **no**:

```
# sshd -T | grep hostbasedauthentication  
hostbasedauthentication no
```

- **IF - Match** set statements are used in your environment, specify the connection parameters to use for the **-T** extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user **sshuser**:*

```
# sshd -T -C user=sshuser | grep hostbasedauthentication
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple **-C** options or as a comma-separated list. The keywords are **addr** (source address), **user** (user), **host** (resolved source host name), **laddr** (local address), **lport** (local port number), and **rdomain** (routing domain)

## Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `HostbasedAuthentication` parameter to `no` above any `Include` and `Match` entries as follows:

```
HostbasedAuthentication no
```

**Note:** First occurrence of a option takes precedence, `Match` set statements withstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

## Default Value:

HostbasedAuthentication no

## References:

1. SSHD\_CONFIG(5)
2. SSHD(8)
3. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1078, T1078.001, T1078.003 | TA0001  | M1042       |



## 5.1.12 Ensure sshd IgnoreRhosts is enabled (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The **IgnoreRhosts** parameter specifies that **.rhosts** and **.shosts** files will not be used in **RhostsRSAAuthentication** or **HostbasedAuthentication**.

### Rationale:

Setting this parameter forces users to enter a password when authenticating with SSH.

### Audit:

Run the following command to verify **IgnoreRhosts** is set to **yes**:

```
# sshd -T | grep ignorerhosts  
ignorerhosts yes
```

- **IF** - **Match** set statements are used in your environment, specify the connection parameters to use for the **-T** extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user **sshuser**:*

```
# sshd -T -C user=sshuser | grep ignorerhosts
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple **-C** options or as a comma-separated list. The keywords are **addr** (source address), **user** (user), **host** (resolved source host name), **laddr** (local address), **lport** (local port number), and **rdomain** (routing domain)

### Remediation:

Edit the **/etc/ssh/sshd\_config** file to set the **IgnoreRhosts** parameter to **yes** above any **Include** and **Match** entries as follows:

```
IgnoreRhosts yes
```

**Note:** First occurrence of a option takes precedence, **Match** set statements withstanding. If **Include** locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in **Include** location.

### Default Value:

IgnoreRhosts yes

## References:

1. SSHD\_CONFIG(5)
2. SSHD(8)
3. NIST SP 800-53 Rev. 5: CM-1,CM-2, CM-6, CM-7, IA-5

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1078, T1078.001, T1078.003 | TA0001  | M1027       |

### 5.1.13 Ensure sshd KexAlgorithms is configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

Key exchange is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received

#### Notes:

- Kex algorithms have a higher preference the earlier they appear in the list
- Some organizations may have stricter requirements for approved Key exchange algorithms
- Ensure that Key exchange algorithms used are in compliance with site policy
- The only Key Exchange Algorithms currently FIPS 140 approved are:
  - ecdh-sha2-nistp256
  - ecdh-sha2-nistp384
  - ecdh-sha2-nistp521
  - diffie-hellman-group-exchange-sha256
  - diffie-hellman-group16-sha512
  - diffie-hellman-group18-sha512
  - diffie-hellman-group14-sha256

#### Rationale:

Key exchange methods that are considered weak should be removed. A key exchange method may be weak because too few bits are used, or the hashing algorithm is considered too weak. Using weak algorithms could expose connections to man-in-the-middle attacks

## Audit:

Run the following command to verify none of the "weak" Key Exchange algorithms are being used:

```
# sshd -T | grep -Pi -- 'kexalgorithms\h+([\^#\n\r]+,)?(diffie-hellman-group1-sha1|diffie-hellman-group14-sha1|diffie-hellman-group-exchange-sha1)\b'
```

Nothing should be returned

The following are considered "weak" Key Exchange Algorithms, and should not be used:

```
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
```

## Remediation:

### Note:

- First occurrence of an option takes precedence.
- Though `key_exchange` may be configured through the `KexAlgorithms` option in the `/etc/ssh/sshd_config` file, it is recommended that the `key_exchange` available to openSSH server are configured through system-wide-crypto-policy
- If the recommendations in the subsection "Configure system wide crypto policy" have been followed, this Audit should be in a passing state. Please review that section before following this Remediation Procedure
- By default, system-wide-crypto-policy is applied to the openSSH server. If the following defaults don't exist due to modifications or upgrade from a earlier release, the system-wide-crypto-policy may not be included by the openSSH server. It is recommended that these defaults be restored, created, or the line `Include /etc/crypto-policies/back-ends/opensshserver.config` be added before any lines containing the `KexAlgorithms` argument.
- Defaults:
  - The file `/etc/ssh/sshd_config` includes the line: `Include /etc/ssh/sshd_config.d/*.conf`. This line must appear before any lines containing the `KexAlgorithms` argument
  - This directory `/etc/ssh/sshd_config.d/` includes a file `/etc/ssh/sshd_config.d/50-redhat.conf`
  - The file `/etc/ssh/sshd_config.d/50-redhat.conf` includes the line `Include /etc/crypto-policies/back-ends/opensshserver.config`
  - The file `/etc/crypto-policies/back-ends/opensshserver.config` is generated by system-wide-crypto-policy

Follow the Remediation Procedure in "Ensure system wide crypto policy disables sha1 hash and signature support"

**This is an excerpt of the Remediation Procedure from "Ensure system wide crypto policy disables sha1 hash and signature support":**

Create or edit a file in `/etc/crypto-policies/policies/modules/` ending in `.pmod` and add or modify the following lines:

```
hash = -SHA1
sign = -*--SHA1
sha1_in_certs = 0
```

*Example:*

```
# printf '%s\n' "# This is a subpolicy dropping the SHA1 hash and signature support" "hash = -SHA1" "sign = -*--SHA1" "sha1_in_certs = 0" >> /etc/crypto-policies/policies/modules/NO-SHA1.pmod
```

Run the following command to update the system-wide cryptographic policy

```
# update-crypto-policies --set
<CRYPTO_POLICY>:<CRYPTO_SUBPOLICY1>:<CRYPTO_SUBPOLICY2>:<CRYPTO_SUBPOLICY3>
```

*Example:*

```
# update-crypto-policies --set DEFAULT:NO-SHA1:NO-WEAKMAC:NO-SSHCBC:NO-SSHCHACHA20:NO-SSHETM:NO-SSHWEAKCIPHERS
```

Run the following command to reload the openSSH server to make your cryptographic settings effective:

```
# systemctl reload-or-restart sshd
```

**- OR -** If system-wide-crypto-policy is not being used to configure available

KexAlgorithms (**This is not recommended**)

Edit the `/etc/ssh/sshd_config` file and add/modify the `KexAlgorithms` line to contain a comma separated list of the site unapproved (weak) KexAlgorithms preceded with a `-` above any `Include` entries:

*Example:*

```
KexAlgorithms -diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1
```

**Default Value:**

KexAlgorithms [sntrup761x25519-sha512@openssh.com](https://ciphersuite.info/docs/openssh-crypto-configuration),curve25519-sha256,[curve25519-sha256@libssh.org](https://ciphersuite.info/docs/libssh.org),ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256

**References:**

1. <https://ubuntu.com/server/docs/openssh-crypto-configuration>
2. NIST SP 800-53 Rev. 5: SC-8
3. SSHD(8)
4. SSHD\_CONFIG(5)

## Additional Information:

The supported algorithms are:

```
curve25519-sha256
curve25519-sha256@libssh.org
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
sntrup4591761x25519-sha512@tinyssh.org
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                         | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |      |    |    |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1040, T1040.000, T1557, T1557.000 | TA0006  | M1041       |

## 5.1.14 Ensure sshd LoginGraceTime is configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The **LoginGraceTime** parameter specifies the time allowed for successful authentication to the SSH server. The longer the Grace period is the more open unauthenticated connections can exist. Like other session controls in this session the Grace Period should be limited to appropriate organizational limits to ensure the service is available for needed access.

### Rationale:

Setting the **LoginGraceTime** parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. It will also limit the number of concurrent unauthenticated connections. While the recommended setting is 60 seconds (1 Minute), set the number based on site policy.

### Audit:

Run the following command and verify that output **LoginGraceTime** is between **1** and **60** seconds:

```
# sshd -T | grep logingracetime  
logingracetime 60
```

### Remediation:

Edit the **/etc/ssh/sshd\_config** file to set the **LoginGraceTime** parameter to **60** seconds or less above any **Include** entry as follows:

```
LoginGraceTime 60
```

**Note:** First occurrence of a option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

### Default Value:

LoginGraceTime 120

**References:**

1. SSHD\_CONFIG(5)
2. NIST SP 800-53 Rev. 5: CM-6
3. SSHD(8)

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques            | Tactics | Mitigations |
|----------------------------------------|---------|-------------|
| T1110, T1110.001, T1110.003, T1110.004 | TA0006  | M1036       |



### 5.1.15 Ensure sshd LogLevel is configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

SSH provides several logging levels with varying amounts of verbosity. The **DEBUG** options are specifically not recommended other than strictly for debugging SSH communications. These levels provide so much data that it is difficult to identify important security information, and may violate the privacy of users.

#### Rationale:

The **INFO** level is the basic level that only records login activity of SSH users. In many situations, such as Incident Response, it is important to determine when a particular user was active on a system. The logout record can eliminate those users who disconnected, which helps narrow the field.

The **VERBOSE** level specifies that login and logout activity as well as the key fingerprint for any SSH key used for login will be logged. This information is important for SSH key management, especially in legacy environments.

#### Audit:

Run the following command and verify that output matches **loglevel VERBOSE** or **loglevel INFO**:

```
# sshd -T | grep loglevel  
  
loglevel VERBOSE  
- OR -  
loglevel INFO
```

- **IF - Match** set statements are used in your environment, specify the connection parameters to use for the **-T** extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user **sshuser**:*

```
# sshd -T -C user=sshuser | grep loglevel
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple **-C** options or as a comma-separated list. The keywords are **addr** (source address), **user** (user), **host** (resolved source host name), **laddr** (local address), **lport** (local port number), and **rdomain** (routing domain)

## Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `LogLevel` parameter to `VERBOSE` or `INFO` above any `Include` and `Match` entries as follows:

```
LogLevel VERBOSE
- OR -
LogLevel INFO
```

**Note:** First occurrence of an option takes precedence, `Match` set statements withstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

## Default Value:

LogLevel INFO

## References:

1. [https://www.ssh.com/ssh/sshd\\_config/](https://www.ssh.com/ssh/sshd_config/)
2. NIST SP 800-53 Rev. 5: AU-3, AU-12, SI-5

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                         | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.2 Collect Audit Logs</b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                         |  |  |  |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          |  |  |  |
| v7               | <b>6.3 Enable Detailed Logging</b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. |                                                                                       |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0005  |             |

### *5.1.16 Ensure sshd MACs are configured (Automated)*

**Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

**Description:**

This variable limits the types of MAC algorithms that SSH can use during communication.

**Notes:**

- Some organizations may have stricter requirements for approved MACs.
- Ensure that MACs used are in compliance with site policy.
- The only "strong" MACs currently FIPS 140 approved are:
  - HMAC-SHA1
  - HMAC-SHA2-256
  - HMAC-SHA2-384
  - HMAC-SHA2-512

**Rationale:**

MD5 and 96-bit MAC algorithms are considered weak and have been shown to increase exploitability in SSH downgrade attacks. Weak algorithms continue to have a great deal of attention as a weak spot that can be exploited with expanded computing power. An attacker that breaks the algorithm could take advantage of a MiTM position to decrypt the SSH tunnel and capture credentials and information.

## Audit:

Run the following command to verify none of the "weak" MACs are being used:

```
# sshd -T | grep -Pi -- 'macs\h+([^\n\r]+,)?(hmac-md5|hmac-md5-96|hmac-ripemd160|hmac-sha1-96|umac-64@openssh\.com|hmac-md5-etm@openssh\.com|hmac-md5-96-etm@openssh\.com|hmac-ripemd160-etm@openssh\.com|hmac-sha1-96-etm@openssh\.com|umac-64-etm@openssh\.com|umac-128-etm@openssh\.com)\b'
```

Nothing should be returned

**Note:** Review [CVE-2023-48795](#) and verify the system has been patched. If the system has not been patched, review the use of the Encrypt Then Mac (etm) MACs. The following are considered "weak" MACs, and should not be used:

```
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-sha1-96
umac-64@openssh.com
hmac-md5-etm@openssh.com
hmac-md5-96-etm@openssh.com
hmac-ripemd160-etm@openssh.com
hmac-sha1-96-etm@openssh.com
umac-64-etm@openssh.com
umac-128-etm@openssh.com
```

## Remediation:

### Note:

- First occurrence of an option takes precedence.
- Though MACs may be configured through the **MACs** option in the `/etc/ssh/sshd_config` file, it is recommended that the MACs available to openSSH server are configured through system-wide-crypto-policy
- If the recommendations in the subsection "Configure system wide crypto policy" have been followed, this Audit should be in a passing state. Please review that section before following this Remediation Procedure
- By default, system-wide-crypto-policy is applied to the openSSH server. If the following defaults don't exist due to modifications or upgrade from a earlier release, the system-wide-crypto-policy may not be included by the openSSH server. It is recommended that these defaults be restored, created, or the line **Include /etc/crypto-policies/back-ends/opensshserver.config** be added before any lines containing the **MACs** argument.

- Defaults:
  - The file `/etc/ssh/sshd_config` includes the line: `Include /etc/ssh/sshd_config.d/*.conf`. This line must appear before any lines containing the `MACs` argument
  - This directory `/etc/ssh/sshd_config.d/` includes a file `/etc/ssh/sshd_config.d/50-redhat.conf`
  - The file `/etc/ssh/sshd_config.d/50-redhat.conf` includes the line `Include /etc/crypto-policies/back-ends/opensshserver.config`
  - The file `/etc/crypto-policies/back-ends/opensshserver.config` is generated by system-wide-crypto-policy

- **IF** - **CVE-2023-48795** has not been reviewed and addressed, Recommendation "Ensure system wide crypto policy disables EtM for ssh" should be followed. Create or edit a file in `/etc/crypto-policies/policies/modules/` ending in `.pmod` and add or modify the the following line:

```
mac@SSH = -HMAC-MD5* -UMAC-64* -UMAC-128*
```

*Example:*

```
# printf '%s\n' "# This is a subpolicy to disable weak MACs" "# for the SSH
protocol (libssh and OpenSSH)" "mac@SSH = -HMAC-MD5* -UMAC-64* -UMAC-128*" >>
/etc/crypto-policies/policies/modules/NO-SSHWEAKMACS.pmod
```

Run the following command to update the system-wide cryptographic policy

```
# update-crypto-policies --set
<CRYPTO_POLICY>:<CRYPTO_SUBPOLICY1>:<CRYPTO_SUBPOLICY2>:<CRYPTO_SUBPOLICY3>
```

*Example:*

```
# update-crypto-policies --set DEFAULT:NO-SHA1:NO-WEAKMAC:NO-SSHCBC:NO-
SSHCHACHA20:NO-SSHETM:NO-SSHWEAKCIPHERS:NO-SSHWEAKMACS
```

Run the following command to reload the openSSH server to make your cryptographic settings effective:

```
# systemctl reload-or-restart sshd
```

- **OR** - If system-wide-crypto-policy is not being used to configure available ciphers (**This is not recommended**)

Edit the `/etc/ssh/sshd_config` file and add/modify the `MACs` line to contain a comma separated list of the site unapproved (weak) MACs preceded with a `-` above any `Include` entries:

*Example:*

```
MACs -hmac-md5,hmac-md5-96,hmac-ripemd160,hmac-sha1-96,umac-
64@openssh.com,hmac-md5-etm@openssh.com,hmac-md5-96-etm@openssh.com,hmac-
ripemd160-etm@openssh.com,hmac-sha1-96-etm@openssh.com,umac-64-
etm@openssh.com,umac-128-etm@openssh.com
```

- **IF** - **CVE-2023-48795** has not been reviewed and addressed, the following `etm` MACs should be added to the exclude list: [hmac-sha1-etm@openssh.com](#),[hmac-sha2-256-etm@openssh.com](#),[hmac-sha2-512-etm@openssh.com](#)

## Default Value:

MACs [umac-64-etm@openssh.com](#), [umac-128-etm@openssh.com](#), [hmac-sha2-256-etm@openssh.com](#), [hmac-sha2-512-etm@openssh.com](#), [hmac-sha1-etm@openssh.com](#), [umac-64@openssh.com](#), [umac-128@openssh.com](#), [hmac-sha2-256](#), [hmac-sha2-512](#), [hmac-sha1](#)

## References:

1. <https://nvd.nist.gov/vuln/detail/CVE-2023-48795>
2. More information on SSH downgrade attacks can be found here: <http://www.mitsl.org/pages/attacks/SLOTH>
3. SSHD\_CONFIG(5)
4. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                         | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).                 |      |    |    |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                                |      |  |  |
| v7               | <b>16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u></b><br>Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels. |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1040, T1040.000, T1557, T1557.000 | TA0006  | M1041       |

### 5.1.17 Ensure sshd MaxAuthTries is configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The **MaxAuthTries** parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the **syslog** file detailing the login failure.

#### Rationale:

Setting the **MaxAuthTries** parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, set the number based on site policy.

#### Audit:

Run the following command and verify that **MaxAuthTries** is 4 or less:

```
# sshd -T | grep maxauthtries  
maxauthtries 4
```

- **IF - Match** set statements are used in your environment, specify the connection parameters to use for the **-T** extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user **ssuser**:*

```
# sshd -T -C user=ssuser | grep maxauthtries
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple **-C** options or as a comma-separated list. The keywords are **addr** (source address), **user** (user), **host** (resolved source host name), **laddr** (local address), **lport** (local port number), and **rdomain** (routing domain)

#### Remediation:

Edit the **/etc/ssh/sshd\_config** file to set the **MaxAuthTries** parameter to 4 or less above any **Include** and **Match** entries as follows:

```
MaxAuthTries 4
```

**Note:** First occurrence of an option takes precedence, **Match** set statements withstanding. If **Include** locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in **Include** location.

**Default Value:**

MaxAuthTries 6

**References:**

1. SSHD\_CONFIG(5)
2. NIST SP 800-53 Rev. 5: AU-3

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      |  |  |
| v7               | <b>16.13 <u>Alert on Account Login Behavior Deviation</u></b><br>Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.                                                                                                                         |      |                                                                                     |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1110, T1110.001, T1110.003 | TA0006  | M1036       |



## 5.1.18 Ensure sshd MaxSessions is configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The **MaxSessions** parameter specifies the maximum number of open sessions permitted from a given connection.

### Rationale:

To protect a system from denial of service due to a large number of concurrent sessions, use the rate limiting function of MaxSessions to protect availability of sshd logins and prevent overwhelming the daemon.

### Audit:

Run the following command and verify that **MaxSessions** is **10** or less:

```
# sshd -T | grep -i maxsessions  
  
maxsessions 10
```

Run the following command and verify the output:

```
grep -Psi -- '^h*MaxSessions\h+\\"?(1[1-9]|[2-9][0-9]|[1-9][0-9][0-9]+)\b'  
/etc/ssh/sshd_config /etc/ssh/sshd_config.d/*.conf  
  
Nothing should be returned
```

- **IF - Match** set statements are used in your environment, specify the connection parameters to use for the **-T** extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user **sshuser**:*

```
# sshd -T -C user=sshuser | grep maxsessions
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple **-C** options or as a comma-separated list. The keywords are **addr** (source address), **user** (user), **host** (resolved source host name), **laddr** (local address), **lport** (local port number), and **rdomain** (routing domain)

## Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `MaxSessions` parameter to **10** or less above any `Include` and `Match` entries as follows:

```
MaxSessions 10
```

**Note:** First occurrence of an option takes precedence, `Match` set statements withstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

## Default Value:

MaxSessions 10

## References:

1. SSHD\_CONFIG(5)
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1499, T1499.002            | TA0040  |             |

## 5.1.19 Ensure sshd MaxStartups is configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The **MaxStartups** parameter specifies the maximum number of concurrent unauthenticated connections to the SSH daemon.

### Rationale:

To protect a system from denial of service due to a large number of pending authentication connection attempts, use the rate limiting function of MaxStartups to protect availability of sshd logins and prevent overwhelming the daemon.

### Audit:

Run the following command to verify **MaxStartups** is **10:30:60** or more restrictive:

```
# sshd -T | awk '$1 ~ /^s*maxstartups/{split($2, a, ":");if(a[1] > 10 || a[2] > 30 || a[3] > 60) print $0}}'
```

Nothing should be returned

### Remediation:

Edit the **/etc/ssh/sshd\_config** file to set the **MaxStartups** parameter to **10:30:60** or more restrictive above any **Include** entries as follows:

```
MaxStartups 10:30:60
```

**Note:** First occurrence of a option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

### Default Value:

MaxStartups 10:30:100

### References:

1. SSHD\_CONFIG(5)
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1499, T1499.002                   | TA0040         |                    |

## 5.1.20 Ensure sshd PermitEmptyPasswords is disabled (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

### Description:

The **PermitEmptyPasswords** parameter specifies if the SSH server allows login to accounts with empty password strings.

### Rationale:

Disallowing remote shell access to accounts that have an empty password reduces the probability of unauthorized access to the system.

### Audit:

Run the following command to verify **PermitEmptyPasswords** is set to **no**:

```
# sshd -T | grep permissemptypasswords  
permissemptypasswords no
```

- **IF - Match** set statements are used in your environment, specify the connection parameters to use for the **-T** extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user **sshuser**:*

```
# sshd -T -C user=sshuser | grep permissemptypasswords
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple **-C** options or as a comma-separated list. The keywords are **addr** (source address), **user** (user), **host** (resolved source host name), **laddr** (local address), **lport** (local port number), and **rdomain** (routing domain)

## Remediation:

Edit `/etc/ssh/sshd_config` and set the `PermitEmptyPasswords` parameter to `no` above any `Include` and `Match` entries as follows:

```
PermitEmptyPasswords no
```

**Note:** First occurrence of an option takes precedence, `Match` set statements withstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location. The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command:

```
# systemctl reload-or-restart sshd.service
```

## Default Value:

`PermitEmptyPasswords no`

## References:

1. SSHD\_CONFIG(5)
2. NIST SP 800-53 Revision 5 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230380  
Rule ID: SV-230380r951612  
STIG ID: RHEL-08-020330  
Severity: CAT I

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                       |  |  |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1021                              | TA0008         | M1042              |

## 5.1.21 Ensure sshd PermitRootLogin is disabled (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

### Description:

The **PermitRootLogin** parameter specifies if the root user can log in using SSH. The default is **prohibit-password**.

### Rationale:

Disallowing **root** logins over SSH requires system admins to authenticate using their own individual account, then escalating to **root**. This limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident.

### Audit:

Run the following command to verify **PermitRootLogin** is set to **no**:

```
# sshd -T | grep permitrootlogin  
  
permitrootlogin no
```

- **IF - Match** set statements are used in your environment, specify the connection parameters to use for the **-T** extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user **sshuser**:*

```
# sshd -T -C user=sshuser | grep permitrootlogin
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple **-C** options or as a comma-separated list. The keywords are **addr** (source address), **user** (user), **host** (resolved source host name), **laddr** (local address), **lport** (local port number), and **rdomain** (routing domain)



## Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `PermitRootLogin` parameter to `no` above any `Include` and `Match` entries as follows:

```
PermitRootLogin no
```

**Note:** First occurrence of an option takes precedence, `Match` set statements withstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

## Default Value:

PermitRootLogin without-password

## References:

1. SSHD\_CONFIG(5)
2. NIST SP 800-53 Rev. 5:AC-6
3. NIST SP 800-53A :: IA-2 (5).2 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230296  
Rule ID: SV-230296r951608  
STIG ID: RHEL-08-010550  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                              | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</b><br>Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. |  |  |  |
| v7               | <b>4.3 Ensure the Use of Dedicated Administrative Accounts</b><br>Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.                     |  |  |  |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1021                              | TA0008         | M1042              |

## 5.1.22 Ensure sshd PermitUserEnvironment is disabled (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

### Description:

The **PermitUserEnvironment** option allows users to present environment options to the SSH daemon.

### Rationale:

Permitting users the ability to set environment variables through the SSH daemon could potentially allow users to bypass security controls (e.g. setting an execution path that has SSH executing trojan'd programs)

### Audit:

Run the following command to verify **PermitUserEnvironment** is set to **no**:

```
# sshd -T | grep permituserenvironment  
permituserenvironment no
```

### Remediation:

Edit the **/etc/ssh/sshd\_config** file to set the **PermitUserEnvironment** parameter to **no** above any **Include** entries as follows:

```
PermitUserEnvironment no
```

**Note:** First occurrence of an option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

### Default Value:

PermitUserEnvironment no

### References:

1. SSHD\_CONFIG(5)
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5
3. SSHD(8)
4. NIST SP 800-53A :: CM-6.1 (iv)

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230330  
Rule ID: SV-230330r951610  
STIG ID: RHEL-08-010830  
Severity: CAT II

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1021                       | TA0008  | M1042       |

### 5.1.23 Ensure sshd UsePAM is enabled (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The **UsePAM** directive enables the Pluggable Authentication Module (PAM) interface. If set to **yes** this will enable PAM authentication using **ChallengeResponseAuthentication** and **PasswordAuthentication** directives in addition to PAM account and session module processing for all authentication types.

#### Rationale:

When **usePAM** is set to **yes**, PAM runs through account and session types properly. This is important if you want to restrict access to services based off of IP, time or other factors of the account. Additionally, you can make sure users inherit certain environment variables on login or disallow access to the server

#### Audit:

Run the following command to verify **UsePAM** is set to **yes**:

```
# sshd -T | grep -i usepam  
usepam yes
```

#### Remediation:

Edit the **/etc/ssh/sshd\_config** file to set the **UsePAM** parameter to **yes** above any **Include** entries as follows:

```
UsePAM yes
```

**Note:** First occurrence of an option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

#### Default Value:

UsePAM yes

#### References:

1. SSHD\_CONFIG(5)
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5
3. SSHD(8)

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1021, T1021.004            | TA0001  | M1035       |

## 5.1.24 Ensure sshd private key files have a passcode (Manual)

### Profile Applicability:

- STIG

### Description:

A private key is a file that helps to enable secure connections through encryption.

### Rationale:

The operating system's certificate-based authentication must enforce authorized access to the corresponding private key.

If an unauthorized user obtains access to a private key without a passcode, that user would have unauthorized access to any system where the associated public key has been installed.

### Audit:

Verify the SSH private key files have a passcode.

For each private key stored on the system, run the following command to verify the SSH private key files have a passcode:

```
# ssh-keygen -y -f </path/to/file>
```

verify the contents of the key are not displayed.

### Remediation:

Run the following command to create a new private and public key pair that utilizes a passcode:

```
# ssh-keygen -n <passphrase>
```

### References:

1. NIST SP 800-53 :: IA-5 (2)
2. NIST SP 800-53A :: IA-5 (2).1

## Additional Information:

### Red Hat Enterprise Linux 8

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230230  
RULE ID: SV-230230r627750  
STIG ID: RHEL-08-010100  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |



## 5.1.25 Ensure sshd X11Forwarding is disabled (Automated)

### Profile Applicability:

- STIG

### Description:

The X11Forwarding parameter provides the ability to tunnel X11 traffic through the connection to enable remote graphic connections.

### Rationale:

Disable X11 forwarding unless there is an operational requirement to use X11 applications directly. There is a small risk that the remote X11 servers of users who are logged in via SSH with X11 forwarding could be compromised by other users on the X11 server. Note that even if X11 forwarding is disabled, users can always install their own forwarders.

### Audit:

Run the following command to verify **x11forwarding** is set to **no**:

```
# sshd -T | grep x11forwarding
x11forwarding no
```

- **IF** - **Match** set statements are used in your environment, specify the connection parameters to use for the **-T** extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user **sshuser**:*

```
# sshd -T -C user=sshuser | grep x11forwarding
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple **-C** options or as a comma-separated list. The keywords are **addr** (source address), **user** (user), **host** (resolved source host name), **laddr** (local address), **lport** (local port number), and **rdomain** (routing domain)

### Remediation:

Edit the **/etc/ssh/sshd\_config** file to set the **X11Forwarding** parameter to **no** above any **Include** and **Match** entries as follows:

```
X11Forwarding no
```

**Note:** First occurrence of a option takes precedence, **Match** set statements withstanding. If **Include** locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in **Include** location.

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230555  
Rule ID: SV-230555r951618  
STIG ID: RHEL-08-040340  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |    |    |
| v7               | <b><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

### *5.1.26 Ensure sshd ClientAliveInterval is configured (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The SSH daemon must be configured with a timeout interval.

#### **Rationale:**

Terminating an idle SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

RHEL 8 operating systems utilize "/etc/ssh/sshd\_config" for configurations of OpenSSH. Within the sshd\_config the product of the values of "ClientAliveInterval" and "ClientAliveCountMax" are used to establish the inactivity threshold. The "ClientAliveInterval" is a timeout interval in seconds after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. The "ClientAliveCountMax" is the number of client alive messages that may be sent without sshd receiving any messages back from the client. If this threshold is met, sshd will disconnect the client. For more information on these settings and others, refer to the "sshd\_config" man pages.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000126-GPOS-00066, SRG-OS-000279-GPOS-00109

## Audit:

Run the following command to verify **ClientAliveInterval** is set to a value of **600** or less:

```
# sshd -T | grep clientalive  
  
ClientAliveInterval 600  
ClientAliveCountMax 0
```

- **IF - Match** set statements are used in your environment, specify the connection parameters to use for the **-T** extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user **sshuser**:*

```
# sshd -T -C user=sshuser | grep clientalive
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple **-C** options or as a comma-separated list. The keywords are **addr** (source address), **user** (user), **host** (resolved source host name), **laddr** (local address), **lport** (local port number), and **rdomain** (routing domain)

## Remediation:

Edit the **/etc/ssh/sshd\_config** file to set the **ClientAliveInterval** parameter to a value of **600** or less above any **Include** and **Match** entries as follows:

```
ClientAliveInterval 600
```

**Note:** First occurrence of a option takes precedence, **Match** set statements withstanding. If **Include** locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in **Include** location. In order for the changes to take effect, the SSH daemon must be restarted.

```
# systemctl reload-or-restart sshd.service
```

## References:

1. NIST SP 800-53 :: SC-10
2. NIST SP 800-53A :: SC-10.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244525  
Rule ID: SV-244525r951596  
STIG ID: RHEL-08-010201  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                      | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.1 <u>Establish and Maintain a Secure Configuration Process</u></b><br>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |
| v7               | <b>16.11 <u>Lock Workstation Sessions After Inactivity</u></b><br>Automatically lock workstation sessions after a standard period of inactivity.                                                                                                                                                                                                                                                                             |  |  |  |

### 5.1.27 Ensure sshd ClientAliveCountMax is configured (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must be configured so that all network connections associated with SSH traffic terminate after becoming unresponsive.

#### Rationale:

Terminating an unresponsive SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, deallocating associated TCP/IP address/port pairs at the operating system level and deallocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean the operating system terminates all sessions or network access; it only ends the unresponsive session and releases the resources associated with that session.

RHEL 8 uses /etc/ssh/sshd\_config for configurations of OpenSSH. Within the sshd\_config, the product of the values of "ClientAliveInterval" and "ClientAliveCountMax" is used to establish the inactivity threshold. The "ClientAliveInterval" is a timeout interval in seconds after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. The "ClientAliveCountMax" is the number of client alive messages that may be sent without sshd receiving any messages back from the client. If this threshold is met, sshd will disconnect the client. For more information on these settings and others, refer to the sshd\_config man pages.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000126-GPOS-00066, SRG-OS-000279-GPOS-00109

#### Impact:

In some cases this setting may cause termination of long-running scripts over SSH or remote automation tools which rely on SSH. In developing the local site policy, the requirements of such scripts should be considered and appropriate ServerAliveInterval and ClientAliveInterval settings should be calculated to insure operational continuity.

## Audit:

Run the following command to verify **ClientAliveCountMax** is set to **1**:

```
# sshd -T | grep clientalivecountmax  
  
clientalivecountmax 1
```

- **IF - Match** set statements are used in your environment, specify the connection parameters to use for the **-T** extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user **sshuser**:*

```
# sshd -T -C user=sshuser | grep clientalivecountmax
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple **-C** options or as a comma-separated list. The keywords are **addr** (source address), **user** (user), **host** (resolved source host name), **laddr** (local address), **lport** (local port number), and **rdomain** (routing domain)

## Remediation:

Edit the **/etc/ssh/sshd\_config** file to set the **ClientAliveCountMax** parameter to **1** above any **Include** and **Match** entries as follows:

```
ClientAliveCountMax 1
```

**Note:** First occurrence of a option takes precedence, **Match** set statements withstanding. If **Include** locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in **Include** location. For the changes to take effect, the SSH daemon must be restarted:

```
# systemctl reload-or-restart sshd.service
```

## Default Value:

ClientAliveInterval 0

ClientAliveCountMax 3

## References:

1. [https://man.openbsd.org/sshd\\_config](https://man.openbsd.org/sshd_config)
2. NIST SP 800-53 Revision 5 :: SC-10
3. NIST SP 800-53A :: SC-10.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230244  
Rule ID: SV-230244r951594  
STIG ID: RHEL-08-010200  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                      | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.1 <u>Establish and Maintain a Secure Configuration Process</u></b><br>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |
| v7               | <b>16.11 <u>Lock Workstation Sessions After Inactivity</u></b><br>Automatically lock workstation sessions after a standard period of inactivity.                                                                                                                                                                                                                                                                             |  |  |  |



### *5.1.28 Ensure the SSH server is configured to use only MACs employing FIPS 140-2-approved algorithms (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The SSH server must be configured to use only Message Authentication Codes (MACs) employing FIPS 140-2 validated cryptographic hash algorithms.

#### **Rationale:**

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

RHEL 8 operating systems incorporate system-wide crypto policies by default. The SSH configuration file has no effect on the ciphers, MACs, or algorithms unless specifically defined in the `/etc/sysconfig/sshd` file. The employed algorithms can be viewed in the `/etc/crypto-policies/back-ends/opensshserver.config` file.

The system will attempt to use the first hash presented by the client that matches the server list. Listing the values "strongest to weakest" is a method to ensure the use of the strongest hash available to secure the SSH connection.

Satisfies: SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174, SRG-OS-000125-GPOS-00065

## Audit:

Verify the SSH server is configured to use only MACs employing FIPS 140-2-approved algorithms with the following command:

```
# grep -i macs /etc/crypto-policies/back-ends/opensshserver.config  
  
-oMACS=hmac-sha2-512,hmac-sha2-256,hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com
```

If the MACs entries in the "opensshserver.config" file have any hashes other than "hmac-sha2-512" and "hmac-sha2-256", the order differs from the example above, they are missing, or commented out, this is a finding.

## Remediation:

Configure the SSH server to use only MACs employing FIPS 140-2-approved algorithms by updating the "/etc/crypto-policies/back-ends/opensshserver.config" file with the following line:

```
-oMACS=hmac-sha2-512,hmac-sha2-256,hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com
```

A reboot is required for the changes to take effect.

## References:

1. NIST SP 800-53 Revision 5 :: AC-17 (2)
2. NIST SP 800-53A :: AC-17 (2).1

## Additional Information:

```
Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024  
  
Vul ID: V-230251  
Rule ID: SV-230251r917870  
STIG ID: RHEL-08-010290  
Severity: CAT II
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                      | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.1 <u>Establish and Maintain a Secure Configuration Process</u></b><br>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                                                                                                                                                                                                                                             |                                                                                     |  |  |
| v7               | <b>16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u></b><br>Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.                                                                                                                                                                                                              |                                                                                     |  |  |

### *5.1.29 Ensure the SSH server is configured to use only ciphers employing FIPS 140-2-approved algorithms (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must implement DoD-approved encryption to protect the confidentiality of SSH server connections.

#### **Rationale:**

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

RHEL 8 operating systems incorporate system-wide crypto policies by default. The SSH configuration file has no effect on the ciphers, MACs, or algorithms unless specifically defined in the `/etc/sysconfig/sshd` file. The employed algorithms can be viewed in the `/etc/crypto-policies/back-ends/opensshserver.config` file.

The system will attempt to use the first hash presented by the client that matches the server list. Listing the values "strongest to weakest" is a method to ensure the use of the strongest hash available to secure the SSH connection.

Satisfies: SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174, SRG-OS-000125-GPOS-00065

## Audit:

Verify the SSH server is configured to use only ciphers employing FIPS 140-2-approved algorithms with the following command:

```
# grep -i ciphers /etc/crypto-policies/back-ends/opensshserver.config  
  
CRYPTO_POLICY='-oCiphers=aes256-ctr,aes192-ctr,aes128-ctr,aes256-  
gcm@openssh.com,aes128-gcm@openssh.com'
```

If the cipher entries in the "opensshserver.config" file have any ciphers other than "aes256-ctr,aes192-ctr,aes128-ctr", the order differs from the example above, they are missing, or commented out, this is a finding.

## Remediation:

Configure the RHEL 8 SSH server to use only ciphers employing FIPS 140-2-approved algorithms by updating the "/etc/crypto-policies/back-ends/opensshserver.config" file with the following line:

```
-oCiphers=aes256-ctr,aes192-ctr,aes128-ctr,aes256-gcm@openssh.com,aes128-  
gcm@openssh.com
```

A reboot is required for the changes to take effect.

## References:

1. NIST SP 800-53 Revision 5 :: AC-17 (2)
2. NIST SP 800-53A :: AC-17 (2).1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024  
  
Vul ID: V-230252  
Rule ID: SV-230252r917873  
STIG ID: RHEL-08-010291  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                         | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |      |  |  |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                |      |  |  |

### 5.1.30 Ensure sshd is configured to use only FIPS-validated key exchange algorithms (Automated)

#### Profile Applicability:

- STIG

#### Description:

SSH server should be configured to use only FIPS-validated key exchange algorithms.

#### Rationale:

Without cryptographic integrity protections provided by FIPS-validated cryptographic algorithms, information can be viewed and altered by unauthorized users without detection.

RHEL 8 incorporates system-wide crypto policies by default. The SSH configuration file has no effect on the ciphers, MACs, or algorithms unless specifically defined in the `/etc/sysconfig/sshd` file. The employed algorithms can be viewed in the `/etc/crypto-policies/back-ends/opensshserver.config` file.

The system will attempt to use the first algorithm presented by the client that matches the server list. Listing the values "strongest to weakest" is a method to ensure the use of the strongest algorithm available to secure the SSH connection.

#### Audit:

Run the following command to verify that the SSH server is configured to use only FIPS-validated key exchange algorithms:

```
# grep -i kexalgorithms /etc/crypto-policies/back-ends/opensshserver.config  
  
CRYPTO_POLICY='-oKexAlgorithms=ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512'
```

If the entries following `KexAlgorithms` have any algorithms defined other than "ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512", appear in different order than shown, or are missing or commented out, this is a finding.

## Remediation:

Edit the `/etc/crypto-policies/back-ends/opensshserver.config` file and add/modify the `KexAlgorithms` to use only FIPS-validated key exchange algorithms:

```
-oKexAlgorithms=ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512
```

A reboot is required for the changes to take effect.

## References:

1. NIST SP 800-53 :: AC-17 (2)
2. NIST SP 800-53A :: AC-17 (2).1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-255924  
Rule ID: SV-255924r917888  
STIG ID: RHEL-08-040342  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                         | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |      | ●    | ●    |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                |      | ●    | ●    |

### 5.1.31 Ensure the SSH server uses strong entropy (Automated)

#### Profile Applicability:

- STIG

#### Description:

Administrators must ensure the SSH server uses strong entropy.

#### Rationale:

The most important characteristic of a random number generator is its randomness, namely its ability to deliver random numbers that are impossible to predict. Entropy in computer security is associated with the unpredictability of a source of randomness. The random source with high entropy tends to achieve a uniform distribution of random values. Random number generators are one of the most important building blocks of cryptosystems.

The SSH implementation in RHEL 8 operating systems uses the OPENSSL library, which does not use high-entropy sources by default. By using the "SSH\_USE\_STRONG\_RNG" environment variable the OPENSSL random generator is reseeded from "/dev/random". This setting is not recommended on computers without the hardware random generator because insufficient entropy causes the connection to be blocked until enough entropy is available.

#### Audit:

Verify the operating system SSH server uses strong entropy with the following command:

**Note:** If the operating system is RHEL versions 8.0 or 8.1, this requirement is not applicable.

```
# grep -i ssh_use_strong_rng /etc/sysconfig/sshd  
SSH_USE_STRONG_RNG=32
```

If the "SSH\_USE\_STRONG\_RNG" line does not equal "32", is commented out or missing, this is a finding.

#### Remediation:

Configure the operating system SSH server to use strong entropy. Add or modify the following line in the "/etc/sysconfig/sshd" file.

```
SSH_USE_STRONG_RNG=32
```

The SSH service must be restarted for changes to take effect.



## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230253  
Rule ID: SV-230253r627750  
STIG ID: RHEL-08-010292  
Severity: CAT III

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                         | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |      |    |    |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                |      |  |  |

### 5.1.32 Ensure sshd StrictModes is enabled (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system's SSH daemon must perform strict mode checking of home directory configuration files.

#### Rationale:

If other users have access to modify user-specific SSH configuration files, they may be able to log on to the system as another user.

#### Audit:

Ensure the SSH daemon performs strict mode checking of home directory configuration files.

Run the following command to verify **StrictModes** is set to **yes**:

```
# sshd -T | grep -i strictmodes  
strictmodes yes
```

If "StrictModes" is set to "no", is missing, or the returned line is commented out, this is a finding.

#### Remediation:

Configure SSH to perform strict mode checking of home directory configuration files. Edit the **/etc/ssh/sshd\_config** file to set the **StrictModes** parameter to **yes** above any **Include** entry as follows:

```
StrictModes yes
```

**Note:** First occurrence of a option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command:

```
# systemctl reload-or-restart sshd.service
```

#### References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230288  
Rule ID: SV-230288r951600  
STIG ID: RHEL-08-010500  
Severity: CAT II

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### *5.1.33 Ensure sshd Banner is configured to display the Standard Mandatory DoD Notice and Consent Banner (Manual)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The **Banner** parameter specifies a file whose contents must be sent to the remote user before authentication is permitted. By default, no banner is displayed.

#### **Rationale:**

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DoD policy

Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

```
I've read & consent to terms in IS user agreem't.
```

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000228-GPOS-00088

### Audit:

Run the following command to verify **Banner** is set:

```
# sshd -T | grep -Pi -- '^banner\h+\|/\H+'
```

*Example:*

```
banner /etc/issue.net
```

- **IF - Match** set statements are used in your environment, specify the connection parameters to use for the **-T** extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user **sshuser**:*

```
# sshd -T -C user=sshuser | grep -Pi -- '^banner\h+\//\H+'
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple **-C** options or as a comma-separated list. The keywords are **addr** (source address), **user** (user), **host** (resolved source host name), **laddr** (local address), **lport** (local port number), and **rdomain** (routing domain).

Run the following command and verify that the contents of the file being called by the **Banner** argument match site policy:

```
# [ -e "$(sshd -T | awk '$1 == "banner" {print $2}')" ] && cat "$(sshd -T | awk '$1 == "banner" {print $2}')"
```

Verify output is:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Run the following command and verify no results are returned:

```
# grep -Psi -- "(\v|r|m|s\b$(grep '^ID=' /etc/os-release | cut -d= -f2 | sed -e 's//g')\b)" "$(sshd -T | awk '$1 == "banner" {print $2}')
```

## Remediation:

Edit the `/etc/ssh/sshd_config` file to set the **Banner** parameter above any **Include** and **Match** entries as follows:

```
Banner /etc/issue.net
```

**Note:** First occurrence of a option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location. Edit the file being called by the **Banner** argument with the appropriate contents according to your site policy:

*Example:*

```
# a_dod_banner=("You are accessing a U.S. Government (USG) Information System
(IS) that is provided for USG-authorized use only." "" "By using this IS
(which includes any device attached to this IS), you consent to the following
conditions:" "" "-The USG routinely intercepts and monitors communications on
this IS for purposes including, but not limited to, penetration" "testing,
COMSEC monitoring, network operations and defense, personnel misconduct (PM),
law enforcement (LE), and" "counterintelligence (CI) investigations." "" "-At
any time, the USG may inspect and seize data stored on this IS." "" "-
Communications using, or data stored on, this IS are not private, are subject
to routine monitoring, interception, and search," "and may be disclosed or
used for any USG-authorized purpose." "" "-This IS includes security measures
(e.g., authentication and access controls) to protect USG interests--not for
your personal" "benefit or privacy." "" "-Notwithstanding the above, using
this IS does not constitute consent to PM, LE or CI investigative searching
or monitoring of" "the content of privileged communications, or work product,
related to personal representation or services by attorneys,"
"psychotherapists, or clergy, and their assistants. Such communications and
work product are private and confidential. See User" "Agreement for
details.")

# printf '%s\n' "${a_dod_banner[@]}" > "$(sshd -T | awk '$1 == "banner"
{print $2}')
```

## References:

1. NIST SP 800-53 :: AC-8 a
2. NIST SP 800-53A :: AC-8.1 (ii)

## Additional Information:

### Red Hat Enterprise Linux 8

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024  
  
GROUP ID: V-230225  
RULE ID: SV-230225r951590  
STIG ID: RHEL-08-010040  
SEVERITY: CAT II

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics        | Mitigations |
|-----------------------------|----------------|-------------|
|                             | TA0001, TA0007 | M1035       |



### 5.1.34 Ensure sshd IgnoreUserKnownHosts is enabled (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system's SSH daemon must not allow authentication using known host's authentication.

#### Rationale:

Configuring this setting for the SSH daemon provides additional assurance that remote login via SSH will require a password, even in the event of misconfiguration elsewhere.

#### Audit:

Verify the SSH daemon does not allow authentication using known host's authentication.

Run the following command to verify **IgnoreUserKnownHosts** is set to **yes**:

```
# sshd -T | grep ignoreuserknownhosts  
  
ignoreuserknownhosts yes
```

If the value is returned as "no", the returned line is commented out, or no output is returned, this is a finding.

#### Remediation:

Configure the SSH daemon to not allow authentication using known host's authentication.

Edit the **/etc/ssh/sshd\_config** file to set the **IgnoreUserKnownHosts** parameter to **yes** above any **Include** entry as follows:

```
IgnoreUserKnownHosts yes
```

**Note:** First occurrence of a option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command:

```
# systemctl reload-or-restart sshd.service
```

#### References:

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230290  
Rule ID: SV-230290r951602  
STIG ID: RHEL-08-010520  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

## 5.1.35 Ensure sshd X11UseLocalhost is enabled (Automated)

### Profile Applicability:

- STIG

### Description:

The SSH daemon must prevent remote hosts from connecting to the proxy display.

### Rationale:

When X11 forwarding is enabled, there may be additional exposure to the server and client displays if the sshd proxy display is configured to listen on the wildcard address. By default, sshd binds the forwarding server to the loopback address and sets the hostname part of the DISPLAY environment variable to localhost. This prevents remote hosts from connecting to the proxy display.

### Audit:

Verify the SSH daemon prevents remote hosts from connecting to the proxy display. Run the following command to verify **X11UseLocalhost** is set to **yes**:

```
# sshd -T | grep x11uselocalhost  
x11uselocalhost yes
```

- **IF - Match** set statements are used in your environment, specify the connection parameters to use for the **-T** extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user **sshuser**:*

```
# sshd -T -C user=sshuser | grep x11uselocalhost
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple **-C** options or as a comma-separated list. The keywords are **addr** (source address), **user** (user), **host** (resolved source host name), **laddr** (local address), **lport** (local port number), and **rdomain** (routing domain)

## Remediation:

Configure the SSH daemon to prevent remote hosts from connecting to the proxy display.

Edit the `/etc/ssh/sshd_config` file to set the `X11UseLocalhost` parameter to `yes` above any `Include` and `Match` entries as follows:

```
X11UseLocalhost yes
```

**Note:** First occurrence of a option takes precedence, `Match` set statements withstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location.

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230556  
Rule ID: SV-230556r951620  
STIG ID: RHEL-08-040341  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### 5.1.36 Ensure sshd KerberosAuthentication is disabled (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system's SSH daemon must not allow Kerberos authentication, except to fulfill documented and validated mission requirements.

#### Rationale:

Configuring these settings for the SSH daemon provides additional assurance that remote logon via SSH will not use unused methods of authentication, even in the event of misconfiguration elsewhere.

#### Audit:

Verify the SSH daemon does not allow Kerberos authentication.

Run the following command to verify **KerberosAuthentication** is set to **no**:

```
# sshd -T | grep kerberosauthentication  
  
kerberosauthentication no
```

- **IF** - **Match** set statements are used in your environment, specify the connection parameters to use for the **-T** extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user **sshuser**:*

```
# sshd -T -C user=sshuser | grep kerberosauthentication
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple **-C** options or as a comma-separated list. The keywords are **addr** (source address), **user** (user), **host** (resolved source host name), **laddr** (local address), **lport** (local port number), and **rdomain** (routing domain). If the value is returned as **yes**, the returned line is commented out, no output is returned, or has not been documented with the ISSO, this is a finding.

Remediation:

Configure the SSH daemon to not allow Kerberos authentication.  
Edit the `/etc/ssh/sshd_config` file to set the `KerberosAuthentication` parameter to `no` above any `Include` and `Match` entries as follows:

```
KerberosAuthentication no
```

**Note:** First occurrence of a option takes precedence, `Match` set statements withstanding. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in `Include` location. The SSH daemon must be restarted for the changes to take effect. To restart the SSH daemon, run the following command:

```
# systemctl reload-or-restart sshd.service
```

References:

- 1. NIST SP 800-53 Revision 5 :: CM-6 b
- 2. NIST SP 800-53A :: CM-6.1 (iv)

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024  
  
Vul ID: V-230291  
Rule ID: SV-230291r952105  
STIG ID: RHEL-08-010521  
Severity: CAT II

CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                     | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | 4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | 9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

### 5.1.37 Ensure sshd RekeyLimit is configured (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must force a frequent session key renegotiation for SSH connections to the server.

**RekeyLimit** Specifies the maximum amount of data that may be transmitted before the session key is renegotiated, optionally followed a maximum amount of time that may pass before the session key is renegotiated. The first argument is specified in bytes and may have a suffix of **K**, **M**, or **G** to indicate Kilobytes, Megabytes, or Gigabytes, respectively. The default is between **1G** and **4G**, depending on the cipher. The optional second value is specified in seconds and may use any of the units documented in the **TIME FORMATS** section. The default value for **RekeyLimit** is default none, which means that rekeying is performed after the cipher's default amount of data has been sent or received and no time based rekeying is done.

#### Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Session key regeneration limits the chances of a session key becoming compromised.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000420-GPOS-00186, SRG-OS-000424-GPOS-00188

## Audit:

Verify the SSH server is configured to force frequent session key renegotiation. Run the following command to verify **RekeyLimit** is set:

```
# sshd -T | grep rekeylimit  
rekeylimit 1G 1h
```

If **RekeyLimit** does not have a maximum data amount and maximum time defined, is missing or commented out, this is a finding.

- **IF - Match** set statements are used in your environment, specify the connection parameters to use for the **-T** extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user **sshuser**:*

```
# sshd -T -C user=sshuser | grep rekeylimit
```

**Note:** If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple **-C** options or as a comma-separated list. The keywords are **addr** (source address), **user** (user), **host** (resolved source host name), **laddr** (local address), **lport** (local port number), and **rdomain** (routing domain)

## Remediation:

Configure the system to force a frequent session key renegotiation for SSH connections to the server.

Edit the **/etc/ssh/sshd\_config** file to set the **RekeyLimit** parameter to **1G 1h** above any **Include** and **Match** entries as follows:

```
RekeyLimit 1G 1h
```

**Note:** First occurrence of a option takes precedence, **Match** set statements withstanding. If **Include** locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in **Include** location. Restart the SSH daemon for the settings to take effect.

```
# systemctl reload-or-restart sshd.service
```

## References:

1. NIST SP 800-53 Revision 5 :: AC-17 (2)
2. NIST SP 800-53A :: AC-17 (2).1



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024  
Vul ID: V-230527  
Rule ID: SV-230527r951616  
STIG ID: RHEL-08-040161  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                         | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |      |  |  |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                |      |  |  |

### 5.1.38 Ensure sshd PrintLastLog is enabled (Automated)

**Profile Applicability:**

- STIG

**Description:**

The operating system must display the date and time of the last successful account logon upon an SSH logon.

**Rationale:**

Providing users with feedback on when account accesses via SSH last occurred facilitates user recognition and reporting of unauthorized account use.

**Audit:**

Verify SSH provides users with feedback on when account accesses last occurred. Run the following command to verify **PrintLastLog** is set to **yes**:

```
# sshd -T | grep -i printlastlog  
printlastlog yes
```

If the "PrintLastLog" keyword is set to "no", is missing, or is commented out, this is a finding.

Remediation:

Configure SSH to provide users with feedback on when account accesses last occurred by setting the required configuration options in "/etc/pam.d/ssh" or in the "sshd\_config" file used by the system ("/etc/ssh/sshd\_config" will be used in the example) (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor).  
Modify the "PrintLastLog" line in "/etc/ssh/sshd\_config" to match the following:

```
PrintLastLog yes
```

Edit the **/etc/ssh/sshd\_config** file to set the **PrintLastLog** parameter to **yes** above any **Include** entry as follows:

```
PrintLastLog yes
```

**Note:** First occurrence of a option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.  
The SSH service must be restarted for changes to "sshd\_config" to take effect.  
Run the following command to restart the ssh daemon service:

```
# systemctl reload-or-restart sshd.service
```

References:

- 1. NIST SP 800-53 Revision 5 :: AC-9
- 2. NIST SP 800-53A :: AC-9.1

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024  
  
Vul ID: V-230382  
Rule ID: SV-230382r951614  
STIG ID: RHEL-08-020350  
Severity: CAT II

CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### 5.1.39 Ensure SSH is loaded and active (Automated)

#### Profile Applicability:

- STIG

#### Description:

All networked systems must have and implement SSH to protect the confidentiality and integrity of transmitted and received information, as well as information during preparation for transmission.

#### Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

#### Audit:

Run the following command to verify SSH is loaded and active:

```
# systemctl list-units | grep sshd.service  
  
sshd.service    loaded active running    OpenSSH server daemon
```

If "sshd" does not show a status of "active" and "running", this is a finding.

## Remediation:

Run the following commands to unmask, enable, and start **sshd.service**:

```
# systemctl unmask sshd.service
# systemctl --now enable sshd.service
```

## References:

1. NIST SP 800-53 Revision 5 :: SC-8

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230526  
Rule ID: SV-230526r916422  
STIG ID: RHEL-08-040160  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                         | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).                 |      | ●    | ●    |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                                |      | ●    | ●    |
| v7               | <b>16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u></b><br>Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels. |      | ●    | ●    |

## 5.2 Configure privilege escalation

There are various tools which allows a permitted user to execute a command as the superuser or another user, as specified by the security policy.

### **sudo**

<https://www.sudo.ws/>

The invoking user's real (not effective) user ID is used to determine the user name with which to query the security policy.

**sudo** supports a plug-in architecture for security policies and input/output logging. Third parties can develop and distribute their own policy and I/O logging plug-ins to work seamlessly with the **sudo** front end. The default security policy is **sudoers**, which is configured via the file **/etc/sudoers** and any entries in **/etc/sudoers.d**.

### **pkexec**

<https://www.freedesktop.org/software/polkit/docs/0.105/pkexec.1.html>

## 5.2.1 Ensure sudo is installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

**sudo** allows a permitted user to execute a command as the superuser or another user, as specified by the security policy. The invoking user's real (not effective) user ID is used to determine the user name with which to query the security policy.

### Rationale:

**sudo** supports a plug-in architecture for security policies and input/output logging. Third parties can develop and distribute their own policy and I/O logging plug-ins to work seamlessly with the **sudo** front end. The default security policy is **sudoers**, which is configured via the file **/etc/sudoers** and any entries in **/etc/sudoers.d**.

The security policy determines what privileges, if any, a user has to run **sudo**. The policy may require that users authenticate themselves with a password or another authentication mechanism. If authentication is required, **sudo** will exit if the user's password is not entered within a configurable time limit. This limit is policy-specific.

### Audit:

Verify that **sudo** is installed.  
Run the following command:

```
# dnf list sudo

Installed Packages
sudo.x86_64          <VERSION>          @anaconda
Available Packages
sudo.x86_64          <VERSION>          updates
```

### Remediation:

Run the following command to install sudo

```
# dnf install sudo
```

### References:

1. SUDO(8)
2. NIST SP 800-53 Rev. 5: AC-6(2), AC-6(5)

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                     | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b><br>Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. |  |  |  |
| v7               | <b><u>4.3 Ensure the Use of Dedicated Administrative Accounts</u></b><br>Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.                     |  |  |  |



## 5.2.2 Ensure the sudoers file has the default include directory (Automated)

### Profile Applicability:

- STIG

### Description:

The default "include" directory should be specified for the `/etc/sudoers` file. It allows adding separate sudo privilege files for specified users or groups, keeping the main sudoers file organized and reducing the risk of error.

### Rationale:

The `sudo` command allows authorized users to run programs (including shells) as other users, system users, and root. The `/etc/sudoers` file is used to configure authorized `sudo` users as well as the programs they are allowed to run. Some configuration options in the `/etc/sudoers` file allow configured users to run programs without re-authenticating. Use of these configuration options makes it easier for one compromised account to be used to compromise other accounts.

It is possible to include other sudoers files from within the sudoers file currently being parsed using the `#include` and `#includedir` directives. When `sudo` reaches this line it will suspend processing of the current file (`/etc/sudoers`) and switch to the specified file/directory. Once the end of the included file(s) is reached, the rest of `/etc/sudoers` will be processed. Files that are included may themselves include other files. A hard limit of 128 nested include files is enforced to prevent include file loops.

### Impact:

If the `include` and `includedir` directives are not present in the `/etc/sudoers` file, this requirement is not applicable.

### Audit:

Run the following command to verify that the `/etc/sudoers` file specifies only the default "include" directory:

```
# grep include /etc/sudoers  
  
/etc/sudoers.d
```

If the results are not `/etc/sudoers.d` or additional files or directories are specified, this is a finding.

Run the following command to ensure the system does not have nested "include" files or directories within the `/etc/sudoers.d` directory:

```
# grep -r include /etc/sudoers.d
```

Nothing should be returned.

Remediation:

Edit the `/etc/sudoers` file to only include the `/etc/sudoers.d` directory with `visudo -f <PATH TO FILE>` and add or modify the following line:

```
#includedir /etc/sudoers.d
```

References:

- 1. NIST SP 800-53 :: CM-6 b
- 2. NIST SP 800-53A :: CM-6.1 (iv)

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-251711  
Rule ID: SV-251711r833385  
STIG ID: RHEL-08-010379  
Severity: CAT II

CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                               | IG 1        | IG 2        | IG 3        |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-------------|-------------|
| v8               | 5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u><br>Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.                                                                  | <div></div> | <div></div> | <div></div> |
| v7               | 4.6 <u>Use of Dedicated Machines For All Administrative Tasks</u><br>Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet. |             |             | <div></div> |

### 5.2.3 Ensure sudo commands use pty (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

**sudo** can be configured to run only from a pseudo terminal (**pseudo-pty**).

#### Rationale:

Attackers can run a malicious program using **sudo** which would fork a background process that remains even when the main program has finished executing.

#### Impact:

**WARNING:** Editing the **sudo** configuration incorrectly can cause **sudo** to stop functioning. Always use **visudo** to modify **sudo** configuration files.

## Audit:

Verify that **sudo** can only run other commands from a pseudo terminal.

Run the following command to verify **Defaults use\_pty** is set:

```
# grep -rPi -- '^h*Defaults\h+([\h*\n\r]+,\h*)?!use_pty\b' /etc/sudoers*
```

Verify the output matches:

```
/etc/sudoers:Defaults use_pty
```

Run the follow command to to verify **Defaults !use\_pty** is not set:

```
# grep -rPi -- '^h*Defaults\h+([\h*\n\r]+,\h*)?!use_pty\b' /etc/sudoers*
```

Nothing should be returned

## Remediation:

Edit the file **/etc/sudoers** with **visudo** or a file in **/etc/sudoers.d/** with **visudo -f <PATH TO FILE>** and add the following line:

```
Defaults use_pty
```

Edit the file **/etc/sudoers** with **visudo** and any files in **/etc/sudoers.d/** with **visudo -f <PATH TO FILE>** and remove any occurrence of **!use\_pty**

## Note:

- sudo will read each file in **/etc/sudoers.d**, skipping file names that end in **~** or contain a **.** character to avoid causing problems with package manager or editor temporary/backup files.
- Files are parsed in sorted lexical order. That is, **/etc/sudoers.d/01\_first** will be parsed before **/etc/sudoers.d/10\_second**.
- Be aware that because the sorting is lexical, not numeric, **/etc/sudoers.d/1\_whoops** would be loaded after **/etc/sudoers.d/10\_second**.
- Using a consistent number of leading zeroes in the file names can be used to avoid such problems.

## References:

1. SUDO(8)
2. VISUDO(8)
3. sudoers(5)
4. NIST SP 800-53 Rev. 5: AC-6

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                     | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b><br>Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. |  |  |  |
| v7               | <b><u>4.3 Ensure the Use of Dedicated Administrative Accounts</u></b><br>Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.                     |  |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics        | Mitigations  |
|------------------------------------|----------------|--------------|
| T1078, T1078.003, T1548, T1548.003 | TA0001, TA0003 | M1026, M1038 |

## 5.2.4 Ensure sudo log file exists (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The **Defaults logfile** entry sets the path to the sudo log file. Setting a path turns on logging to a file; negating this option turns it off. By default, sudo logs via syslog.

### Rationale:

Defining a dedicated log file for sudo simplifies auditing of sudo commands and creation of auditd rules for sudo.

### Impact:

**WARNING:** Editing the **sudo** configuration incorrectly can cause **sudo** to stop functioning. Always use **visudo** to modify **sudo** configuration files.

Creation of additional log files can cause disk space exhaustion if not correctly managed. You should configure **logrotate** to manage the sudo log in accordance with your local policy.

### Audit:

Run the following command to verify that sudo has a custom log file configured

```
# grep -rPsi  
"^\\h*Defaults\\h+([\\^#]+,\\h*)?logfile\\h*=\\h*(\\\"|\\')?\\H+(\\\"|\\')?(,\\h*\\H+\\h*)*\\h*  
(#.*)?$" /etc/sudoers*
```

### Example output:

```
Defaults logfile="/var/log/sudo.log"
```

## Remediation:

Edit the file `/etc/sudoers` or a file in `/etc/sudoers.d/` with `visudo -f <PATH TO FILE>` and add the following line:

```
Defaults logfile="<PATH TO CUSTOM LOG FILE>"
```

### Example

```
Defaults logfile="/var/log/sudo.log"
```

## Notes:

- `sudo` will read each file in `/etc/sudoers.d`, skipping file names that end in `~` or contain a `.` character to avoid causing problems with package manager or editor temporary/backup files.
- Files are parsed in sorted lexical order. That is, `/etc/sudoers.d/01_first` will be parsed before `/etc/sudoers.d/10_second`.
- Be aware that because the sorting is lexical, not numeric, `/etc/sudoers.d/1_whoops` would be loaded after `/etc/sudoers.d/10_second`.
- Using a consistent number of leading zeroes in the file names can be used to avoid such problems.

## References:

1. SUDO(8)
2. VISUDO(8)
3. sudoers(5)
4. NIST SP 800-53 Rev. 5: AU-3, AU-12

## Additional Information:

`visudo` edits the `sudoers` file in a safe fashion, analogous to `vipw(8)`. `visudo` locks the `sudoers` file against multiple simultaneous edits, provides basic sanity checks, and checks for parse errors. If the `sudoers` file is currently being edited you will receive a message to try again later.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      |  |  |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.                                                                                |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0004  | M1026       |



## 5.2.5 Ensure users must provide password for escalation (Automated)

### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG

### Description:

The operating system must be configured so that users must provide a password for privilege escalation.

### Rationale:

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user re-authenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

### Impact:

This will prevent automated processes from being able to elevate privileges.

### Audit:

**Note:** If passwords are not being used for authentication, this is not applicable. Verify the operating system requires users to supply a password for privilege escalation. Check the configuration of the `/etc/sudoers` and `/etc/sudoers.d/*` files with the following command:

```
# grep -r "^[^#]*NOPASSWD" /etc/sudoers*
```

If any line is found refer to the remediation procedure below.

### Remediation:

Based on the outcome of the audit procedure, use `visudo -f <PATH TO FILE>` to edit the relevant sudoers file.

Remove any line with occurrences of `NOPASSWD` tags in the file.

### References:

1. NIST SP 800-53 Rev. 5: AC-6

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230271  
Rule ID: SV-230271r854026  
STIG ID: RHEL-08-010380  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                     | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b><br>Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. |  |  |  |
| v7               | <b><u>4.3 Ensure the Use of Dedicated Administrative Accounts</u></b><br>Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.                     |  |  |  |

## 5.2.6 Ensure the sudoers file restricts sudo access to authorized personnel (Automated)

### Profile Applicability:

- STIG

### Description:

The operating system must restrict privilege elevation to authorized personnel.

### Rationale:

The sudo command allows a user to execute programs with elevated (administrator) privileges. It prompts the user for their password and confirms your request to execute a command by checking a file, called sudoers. If the "sudoers" file is not configured correctly, any user defined on the system can initiate privileged actions on the target system.

### Audit:

Verify the "sudoers" file restricts sudo access to authorized personnel:

```
# grep -iw 'ALL' /etc/sudoers /etc/sudoers.d/*
```

If the either of the following entries are returned, this is a finding:

```
ALL ALL=(ALL) ALL
ALL ALL=(ALL:ALL) ALL
```

### Remediation:

Remove the following entries from the sudoers file:

```
ALL ALL=(ALL) ALL
ALL ALL=(ALL:ALL) ALL
```

### References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-237641  
Rule ID: SV-237641r646893  
STIG ID: RHEL-08-010382  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                     | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b><br>Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. |  |  |  |
| v7               | <b><u>4.3 Ensure the Use of Dedicated Administrative Accounts</u></b><br>Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.                     |  |  |  |

## *5.2.7 Ensure re-authentication for privilege escalation is not disabled globally (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation
- STIG

### **Description:**

The operating system must be configured so that users must re-authenticate for privilege escalation.

### **Rationale:**

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user re-authenticate.

### **Audit:**

Verify the operating system requires users to re-authenticate for privilege escalation. Check the configuration of the `/etc/sudoers` and `/etc/sudoers.d/*` files with the following command:

```
# grep -r "^[^#].*\!authenticate" /etc/sudoers*
```

If any line is found with a `!authenticate` tag, refer to the remediation procedure below.

### **Remediation:**

Configure the operating system to require users to reauthenticate for privilege escalation.

Based on the outcome of the audit procedure, use `visudo -f <PATH TO FILE>` to edit the relevant sudoers file.

Remove any occurrences of `!authenticate` tags in the file(s).

### **References:**

1. NIST SP 800-53 Rev. 5: AC-6

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230272  
Rule ID: SV-230272r854027  
STIG ID: RHEL-08-010381  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                     | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b><br>Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. |  |  |  |
| v7               | <b><u>4.3 Ensure the Use of Dedicated Administrative Accounts</u></b><br>Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.                     |  |  |  |

## 5.2.8 Ensure the sudoers security policy is configured to use the invoking user's password for privilege escalation (Automated)

### Profile Applicability:

- STIG

### Description:

The operating system must use the invoking user's password for privilege escalation when using "sudo".

### Rationale:

The sudoers security policy requires that users authenticate themselves before they can use sudo. When sudoers requires authentication, it validates the invoking user's credentials. If the rootpw, targetpw, or runaspw flags are defined and not disabled, by default the operating system will prompt the invoking user for the "root" user password.

For more information on each of the listed configurations, reference the sudoers(5) manual page.

### Audit:

Verify that the sudoers security policy is configured to use the invoking user's password for privilege escalation.

```
# grep -E '(!rootpw|!targetpw|!runaspw)' /etc/sudoers /etc/sudoers.d/* | grep -v '#'

/etc/sudoers:Defaults !targetpw
/etc/sudoers:Defaults !rootpw
/etc/sudoers:Defaults !runaspw
```

If no results are returned, this is a finding.

If "Defaults !targetpw" is not defined, this is a finding.

If "Defaults !rootpw" is not defined, this is a finding.

If "Defaults !runaspw" is not defined, this is a finding.

### Remediation:

Define the following in the Defaults section of the `/etc/sudoers` file or a configuration file in the `/etc/sudoers.d/` directory:

```
Defaults !targetpw
Defaults !rootpw
Defaults !runaspw
```

Remove any configurations that conflict with the above from the following locations:

`/etc/sudoers`

`/etc/sudoers.d/`

## References:

1. NIST SP 800-53 Revision 5 :: AC-6 (5)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-237642  
Rule ID: SV-237642r880727  
STIG ID: RHEL-08-010383  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                       | IG 1                                                                                | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u></b><br>Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. |  |    |    |
| v7               | <b>5.4 <u>Deploy System Configuration Management Tools</u></b><br>Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.                                                                                               |                                                                                     |  |  |



## 5.2.9 Ensure sudo timestamp\_timeout is configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

### Description:

**sudo** caches used credentials for a default of 5 minutes. This is for ease of use when there are multiple administrative tasks to perform. The timeout can be modified to suit local security policies.

### Rationale:

Setting a timeout value reduces the window of opportunity for unauthorized privileged access to another user.

### Audit:

Ensure that the caching timeout is no more than 15 minutes.

#### Example:

```
# grep -roP "timestamp_timeout=\K[0-9]*" /etc/sudoers*
```

If there is no **timestamp\_timeout** configured in **/etc/sudoers\*** then the default is 5 minutes. This default can be checked with:

```
# sudo -V | grep "Authentication timestamp timeout:"
```

**Note:** A value of **-1** means that the timeout is disabled. Depending on the configuration of the **timestamp\_type**, this could mean for all terminals / processes of that user and not just that one single terminal session.

### Remediation:

If the currently configured timeout is larger than 15 minutes, edit the file listed in the audit section with **visudo -f <PATH TO FILE>** and modify the entry **timestamp\_timeout=** to 15 minutes or less as per your site policy. The value is in minutes. This particular entry may appear on its own, or on the same line as **env\_reset**. See the following two examples:

```
Defaults    env_reset, timestamp_timeout=15
Defaults    timestamp_timeout=15
Defaults    env_reset
```

## References:

1. <https://www.sudo.ws/man/1.9.0/sudoers.man.html>
2. NIST SP 800-53 Revision 4 :: IA-11

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-237643  
Rule ID: SV-237643r861088  
STIG ID: RHEL-08-010384  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                     | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b><u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b><br>Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. |    |    |    |
| v7               | <b><u>4.3 Ensure the Use of Dedicated Administrative Accounts</u></b><br>Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.                     |  |  |  |

## 5.2.10 Ensure access to the su command is restricted (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The **su** command allows a user to run a command or shell as another user. The program has been superseded by **sudo**, which allows for more granular control over privileged access. Normally, the **su** command can be executed by any user. By uncommenting the **pam\_wheel.so** statement in **/etc/pam.d/su**, the **su** command will only allow users in a specific groups to execute **su**. This group should be empty to reinforce the use of **sudo** for privileged access.

### Rationale:

Restricting the use of **su**, and using **sudo** in its place, provides system administrators better control of the escalation of user privileges to execute privileged commands. The **sudo** utility also provides a better logging and audit mechanism, as it can log each command executed via **sudo**, whereas **su** can only record that a user executed the **su** program.

### Audit:

Run the following command and verify the output matches the line:

```
# grep -Pi
'^\h*auth\h+(?:required|requisite)\h+pam_wheel\.so\h+(?:[^\n\r]+\h+)?((?!2)
(use_uid\b|group=\H+\b))\h+(?:[^\n\r]+\h+)?((?!1)(use_uid\b|group=\H+\b))(\
h+\.*)?$' /etc/pam.d/su

auth required pam_wheel.so use_uid group=<group_name>
```

Run the following command and verify that the group specified in **<group\_name>** contains no users:

```
# grep <group_name> /etc/group

<group_name>:x:<GID>:
```

There should be no users listed after the Group ID field.

## Remediation:

Create an empty group that will be specified for use of the **su** command. The group should be named according to site policy.

*Example:*

```
# groupadd sugroup
```

Add the following line to the **/etc/pam.d/su** file, specifying the empty group:

```
auth required pam_wheel.so use_uid group=sugroup
```

## References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |    |    |    |
| v7               | <b>14.6 Protect Information through Access Control Lists</b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1078                       | TA0005  | M1026       |

### 5.2.11 Ensure `pam_succeed_if` does not exist in `/etc/pam.d/sudo` (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system (OS) must not be configured to bypass password requirements for privilege escalation.

#### Rationale:

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user re-authenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

#### Audit:

Verify the operating system is not be configured to bypass password requirements for privilege escalation.

Check the configuration of the `/etc/pam.d/sudo` file with the following command:

```
# grep pam_succeed_if /etc/pam.d/sudo
```

If any occurrences of `"pam_succeed_if"` is returned from the command, this is a finding.

#### Remediation:

Configure the operating system to require users to supply a password for privilege escalation.

Check the configuration of the `/etc/pam.d/sudo` file with the following command:

```
# vi /etc/pam.d/sudo
```

Remove any occurrences of `"pam_succeed_if"` in the file.

#### References:

1. NIST SP 800-53 Revision 4 :: IA-11

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-251712  
RULE ID: SV-251712r854083  
STIG ID: RHEL-08-010385  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                     | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b><br>Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. |  |  |  |
| v7               | <b><u>4.3 Ensure the Use of Dedicated Administrative Accounts</u></b><br>Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.                     |  |  |  |

## 5.3 Pluggable Authentication Modules

Pluggable Authentication Modules (PAM) is a service that implements modular authentication modules on UNIX systems. PAM is implemented as a set of shared objects that are loaded and executed when a program needs to authenticate a user. Files for PAM are typically located in the `/etc/pam.d` directory. PAM must be carefully configured to secure system authentication. While this section covers some of PAM, please consult other PAM resources to fully understand the configuration capabilities.

### **5.3.1 Configure PAM software packages**

Updated versions of PAM and authselect include additional functionality



### 5.3.1.1 Ensure latest version of pam is installed (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

Updated versions of PAM include additional functionality

#### Rationale:

To ensure the system has full functionality and access to the options covered by this Benchmark, pam-1.3.1-25 or latter is required

#### Audit:

Run the following command to verify the version of **PAM** on the system:

```
# rpm -q pam
```

The output should be similar to:

```
pam-1.3.1-25.el8.x86_64
```

#### Remediation:

- **IF** - the version of **PAM** on the system is less that version **pam-1.3.1-25**:

Run the following command to update to the latest version of **PAM**:

```
# dnf upgrade pam
```

### *5.3.1.2 Ensure latest version of authselect is installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Authselect is a utility that simplifies the configuration of user authentication. Authselect offers ready-made profiles that can be universally used with all modern identity management systems

You can create and deploy a custom profile by customizing one of the default profiles, the sssd, winbind, or the nis profile. This is particularly useful if Modifying a ready-made authselect profile is not enough for your needs. When you deploy a custom profile, the profile is applied to every user logging into the given host. This would be the recommended method, so that the existing profiles can remain unmodified.

Updated versions of **authselect** include additional functionality

#### **Rationale:**

Authselect makes testing and troubleshooting easy because it only modifies files in these directories:

- **/etc/nsswitch.conf**
- **/etc/pam.d/\***
- **/etc/dconf/db/distro.d/\***

To ensure the system has full functionality and access to the options covered by this Benchmark, **authselect-1.2.6-1** or latter is required

**Impact:**

If local site customizations have been made to an authselect default or custom profile created with the `--symlink-pam` option, these customizations may be over-written by updating authselect.

**WARNING:**

Do not use authselect if:

- your host is part of Linux Identity Management. Joining your host to an IdM domain with the `ipa-client-install` command automatically configures SSSD authentication on your host.
- Your host is part of Active Directory via SSSD. Calling the `realm join` command to join your host to an Active Directory domain automatically configures SSSD authentication on your host.

It is **not** recommended to change the authselect profiles configured by `ipa-client-install` or `realm join`. If you need to modify them, display the current settings before making any modifications, so you can revert back to them if necessary

**Audit:**

Run the following command to verify the version of `authselect` on the system:

```
# rpm -q authselect
```

The output should be similar to:

```
authselect-1.2.6-1.el8.x86_64
```

**Remediation:**

Run the following command to install `authselect`:

```
# dnf install authselect
```

- **IF** - the version of `authselect` on the system is less than version `authselect-1.2.6-1`:

Run the following command to update to the latest version of `authselect`:

```
# dnf upgrade authselect
```

## 5.3.2 Configure authselect

Authselect is a utility that simplifies the configuration of user authentication. Authselect offers ready-made profiles that can be universally used with all modern identity management systems

Authselect makes testing and troubleshooting easy because it only modifies files in these directories:

- `/etc/nsswitch.conf`
- `/etc/pam.d/*` files
- `/etc/dconf/db/distro.d/*` files

You can create and deploy a custom profile by customizing one of the default profiles, the sssd, winbind, or the nis profile. This is particularly useful if Modifying a ready-made authselect profile is not enough for your needs. When you deploy a custom profile, the profile is applied to every user logging into the given host. This would be the recommended method, so that the existing profiles can remain unmodified.

Profile Directories - Profiles can be found in one of three directories:

- `/usr/share/authselect/default` - Read-only directory containing profiles shipped together with authselect.
- `/usr/share/authselect/vendor` - Read-only directory for vendor-specific profiles that can override the ones in default directory.
- `/etc/authselect/custom` - Place for administrator-defined profiles.

Profile Files - Each profile consists of one or more of these files which provide a mandatory profile description and describe the changes that are done to the system:

- `README` - Description of the profile. The first line must be a name of the profile.
- `system-auth` - PAM stack that is included from nearly all individual service configuration files.
- `password-auth`, `smartcard-auth`, `fingerprint-auth` - These PAM stacks are for applications which handle authentication from different types of devices via simultaneously running individual conversations instead of one aggregate conversation.
- `postlogin` - The purpose of this PAM stack is to provide a common place for all PAM modules which should be called after the stack configured in `system-auth` or the other common PAM configuration files. It is included from all individual service configuration files that provide login service with shell or file access.  
**Note:** the modules in the postlogin configuration file are executed regardless of the success or failure of the modules in the `system-auth` configuration file.
- `nsswitch.conf` - Name Service Switch configuration file. Only maps relevant to the profile must be set. Maps that are not specified by the profile are included from `/etc/authselect/user-nsswitch.conf`.

- **dconf-db** - Changes to dconf database. The main use case of this file is to set changes for gnome login screen in order to enable or disable smartcard and fingerprint authentication.
- **dconf-locks** - This file defines locks on values set in dconf database.

Conditional lines - Each of these files serves as a template. A template is a plain text file with optional usage of several operators that can be used to provide some optional profile features.

- **{continue if "feature"}** - Immediately stop processing of the file unless "feature" is defined (the rest of the file content will be removed). If "feature" is defined, the whole line with this operator will be removed and the rest of the template will be processed.
- **{stop if "feature"}** - Opposite of "continue if". Immediately stop processing of the file if "feature" is defined (the rest of the file content will be removed). If "feature" is not defined, the whole line with this operator will be removed and the rest of the template will be processed.
- **{include if "feature"}** - Include the line where this operator is placed only if "feature" is defined.
- **{exclude if "feature"}** - Opposite to "include-if". Include the line where this operator is placed only if "feature" is not defined.
- **{imply "implied-feature" if "feature"}** - Enable feature "implied-feature" if feature "feature" is enabled. The whole line with this operator is removed, thus it is not possible to add anything else around this operator at the same line.
- **{if "feature":true|false}** - If "feature" is defined, replace this operator with string "true", otherwise with string "false".
- **{if "feature":true}** - If "feature" is defined, replace this operator with string "true", otherwise with an empty string.

*Example of creating a custom authselect profile called custom-profile*

```
# authselect create-profile custom-profile -b sssd
```

## **WARNING:**

Do not use authselect if:

- Your host is part of Linux Identity Management. Joining your host to an IdM domain with the ipa-client-install command automatically configures SSSD authentication on your host.
- Your host is part of Active Directory via SSSD. Calling the realm join command to join your host to an Active Directory domain automatically configures SSSD authentication on your host.
- It is not recommended to change the authselect profiles configured by ipa-client-install or realm join. If you need to modify them, display the current settings before making any modifications, so you can revert back to them if necessary.

### 5.3.2.1 Ensure active authselect profile includes pam modules (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

A custom profile can be created by copying and customizing one of the default profiles. The default profiles include: sssd, winbind, and nis. These profile can be customized to follow site specific requirements.

You can select a profile for the authselect utility for a specific host. The profile will be applied to every user logging into the host.

#### Rationale:

A custom profile is required to customize many of the pam options.

Modifications made to a default profile may be overwritten during an update.

When you deploy a profile, the profile is applied to every user logging into the given host

#### Impact:

If local site customizations have been made to the authselect template or files in `/etc/pam.d` these custom entries should be added to the newly created custom profile before it's applied to the system.

**Note:** The order within the pam stacks is important when adding these entries. Specifically for the password stack, the `use_authtok` option is important, and should appear on all modules except for the first entry.

#### Example:

```
password requisite pam_pwquality.so local_users_only #<-- Top of password
stack, doesn't include use_authtok
password required pam_pwhistory.so use_authtok #<-- subsequent entry in
password stack, includes use_authtok
```

## Audit:

Run the following command to verify the active authselect profile includes lines for the **pwquality**, **pwhistory**, **faillock**, and **unix** modules:

```
# grep -P --
'\b(pam_pwquality\.so|pam_pwhistory\.so|pam_faillock\.so|pam_unix\.so)\b'
/etc/authselect/"$(head -1
/etc/authselect/authselect.conf)"/{system,password}-auth
```

### Example output:

```
/etc/authselect/custom/custom-profile/password-auth:auth      required    pam_faillock.so
preauth silent {include if "with-faillock"}
/etc/authselect/custom/custom-profile/password-auth:auth      sufficient  pam_unix.so
{if not "without-nullok":nullok}
/etc/authselect/custom/custom-profile/password-auth:auth      required    pam_faillock.so
authfail {include if "with-faillock"}

/etc/authselect/custom/custom-profile/password-auth:account    required
pam_faillock.so {include if "with-faillock"}
/etc/authselect/custom/custom-profile/password-auth:account    required    pam_unix.so

/etc/authselect/custom/custom-profile/password-auth:password   requisite
pam_pwquality.so local_users_only
/etc/authselect/custom/custom-profile/password-auth:password   required
pam_pwhistory.so use_authtok
/etc/authselect/custom/custom-profile/password-auth:password   sufficient  pam_unix.so
sha512 shadow {if not "without-nullok":nullok} use_authtok

/etc/authselect/custom/custom-profile/password-auth:session    required    pam_unix.so

/etc/authselect/custom/custom-profile/system-auth:auth         required    pam_faillock.so
preauth silent {include if "with-faillock"}
/etc/authselect/custom/custom-profile/system-auth:auth         sufficient  pam_unix.so {if
not "without-nullok":nullok}
/etc/authselect/custom/custom-profile/system-auth:auth         required    pam_faillock.so
authfail {include if "with-faillock"}

/etc/authselect/custom/custom-profile/system-auth:account      required    pam_faillock.so
{include if "with-faillock"}
/etc/authselect/custom/custom-profile/system-auth:account      required    pam_unix.so

/etc/authselect/custom/custom-profile/system-auth:password     requisite
pam_pwquality.so local_users_only
/etc/authselect/custom/custom-profile/system-auth:password     required
pam_pwhistory.so use_authtok
/etc/authselect/custom/custom-profile/system-auth:password     sufficient  pam_unix.so
sha512 shadow {if not "without-nullok":nullok}

/etc/authselect/custom/custom-profile/system-auth:session      required    pam_unix.so
```

## Notes:

- The lines may or may not include feature options defined by text surrounded by curly brackets ({}), e.g. **{include if "with-faillock"}**
- File path may be different due to the active profile in use

## Remediation:

Perform the following to create a custom authselect profile, with the modules covered in this Benchmark correctly included in the custom profile template files

Run the following command to create a custom authselect profile:

```
# authselect create-profile <custom-profile name> <options>
```

*Example:*

```
# authselect create-profile custom-profile -b sssd
```

Run the following command to select a custom authselect profile:

```
# authselect select custom/<CUSTOM PROFILE NAME> {with-<OPTIONS>} {--force}
```

*Example:*

```
# authselect select custom/custom-profile --backup=PAM_CONFIG_BACKUP --force
```

### Notes:

- The PAM and authselect packages must be versions **pam-1.3.1-25** and **authselect-1.2.6-1** or newer
- The example is based on a custom profile built (copied) from the the **SSSD** default authselect profile.
- The example does not include the **symlink** option for the **PAM** or **Metadata** files. This is due to the fact that by linking the **PAM** files future updates to **authselect** may overwrite local site customizations to the custom profile
- The **--backup=PAM\_CONFIG\_BACKUP** option will create a backup of the current config. The backup will be stored at **/var/lib/authselect/backups/PAM\_CONFIG\_BACKUP**
- The **--force** option will force the overwrite of the existing files and automatically backup system files before writing any change unless the **--nobackup** option is set.
  - On a new system where authselect has not been configured. In this case, the **--force** option will force the selected authselect profile to be active and overwrite the existing files with files generated from the selected authselect profile's templates
  - On an existing system with a custom configuration. The **--force** option may be used, but **ensure that you note the backup location included as your custom files will be overwritten.** This will allow you to review the changes and add any necessary customizations to the template files for the authselect profile. After updating the templates, run the command **authselect apply-changes** to add these custom entries to the files in **/etc/pam.d/**

**- IF -** you receive an error ending with a message similar to:

```
[error] Refusing to activate profile unless those changes are removed or
overwrite is requested.
Some unexpected changes to the configuration were detected. Use 'select'
command instead.
```

This error is caused when the previous configuration was not created by authselect but by other tool or by manual changes and the **--force** option will be required to enable the authselect profile.



## References:

1. authselect(8)
2. [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/9/html/configuring\\_authentication\\_and\\_authorization\\_in\\_rhel/configuring-user-authentication-using-authselect\\_configuring-authentication-and-authorization-in-rhel#creating-and-deploying-your-own-authselect-profile\\_configuring-user-authentication-using-authselect](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/configuring_authentication_and_authorization_in_rhel/configuring-user-authentication-using-authselect_configuring-authentication-and-authorization-in-rhel#creating-and-deploying-your-own-authselect-profile_configuring-user-authentication-using-authselect)
3. <https://docs.oracle.com/en/operating-systems/oracle-linux/9/userauth/OL9-USERAUTH.pdf>

## Additional Information:

with the option `--base-on=BASE-ID` or `-b=BASE-ID` the new profile will be based on a profile named BASE-ID.

The base profile location is determined with these steps:

1. If BASE-ID starts with prefix custom/ it is a custom profile.
2. Try if BASE-ID is found in vendor profiles.
3. Try if BASE-ID is found in default profiles.
4. Return an error.

The authselect option `--force` or `-f` will cause authselect to write changes even if the previous configuration was not created by authselect but by other tool or by manual changes. This option will automatically backup system files before writing any change unless the `--nobackup` option is set.

### *Example:*

```
authselect select custom/custom-profile with-pwhistory with-faillock without-  
nullok --backup=PAM_CONFIG_BACKUP --force
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <p><b><u>16.2 Establish and Maintain a Process to Accept and Address Software Vulnerabilities</u></b></p> <p>Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.</p> |      |  |  |
| v7               | <p><b><u>16.7 Establish Process for Revoking Access</u></b></p> <p>Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |      |  |  |

### 5.3.2.2 Ensure pam\_faillock module is enabled (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The **pam\_faillock.so** module maintains a list of failed authentication attempts per user during a specified interval and locks the account in case there were more than the configured number of consecutive failed authentications (this is defined by the **deny** parameter in the faillock configuration). It stores the failure records into per-user files in the tally directory.

#### Rationale:

Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

#### Audit:

Run the following commands to verify that **pam\_faillock** is enabled

```
# grep -P -- '\bpam_faillock.so\b' /etc/pam.d/{password,system}-auth
```

Output should be similar to:

|                                  |          |                          |
|----------------------------------|----------|--------------------------|
| /etc/pam.d/password-auth:auth    | required | pam_faillock.so preauth  |
| silent                           |          |                          |
| /etc/pam.d/password-auth:auth    | required | pam_faillock.so authfail |
| /etc/pam.d/password-auth:account | required | pam_faillock.so          |
| /etc/pam.d/system-auth:auth      | required | pam_faillock.so preauth  |
| silent                           |          |                          |
| /etc/pam.d/system-auth:auth      | required | pam_faillock.so authfail |
| /etc/pam.d/system-auth:account   | required | pam_faillock.so          |

## Remediation:

Run the following script to verify the `pam_faillock.so` lines exist in the profile templates:

```
#!/usr/bin/env bash

{
  l_module_name="faillock"
  l_pam_profile="$(head -1 /etc/authselect/authselect.conf)"
  if grep -Pq -- '^custom\/' <<< "$l_pam_profile"; then
    l_pam_profile_path="/etc/authselect/$l_pam_profile"
  else
    l_pam_profile_path="/usr/share/authselect/default/$l_pam_profile"
  fi
  grep -P -- "\bpam_$l_module_name\.so\b"
  "$l_pam_profile_path"/{password,system}-auth
}
```

*Example Output with a custom profile named "custom-profile":*

```
/etc/authselect/custom/custom-profile/password-auth:auth    required
pam_faillock.so preauth silent {include if "with-faillock"}
/etc/authselect/custom/custom-profile/password-auth:auth    required
pam_faillock.so authfail {include if "with-faillock"}
/etc/authselect/custom/custom-profile/password-auth:account  required
pam_faillock.so {include if "with-faillock"}

/etc/authselect/custom/custom-profile/system-auth:auth      required
pam_faillock.so preauth silent {include if "with-faillock"}
/etc/authselect/custom/custom-profile/system-auth:auth      required
pam_faillock.so authfail {include if "with-faillock"}
/etc/authselect/custom/custom-profile/system-auth:account   required
pam_faillock.so {include if "with-faillock"}
```

**Note:** The lines may not include `{include if "with-faillock"}`

- **IF** - the lines shown above are not returned, refer to the Recommendation "Ensure active authselect profile includes pam modules" to update the authselect profile template files to include the `pam_faillock` entries before continuing this remediation.
- **IF** - the lines include `{include if "with-faillock"}`, run the following command to enable the authselect `with-faillock` feature and update the files in `/etc/pam.d` to include `pam_faillock.so`:

```
# authselect enable-feature with-faillock
```

- **IF** - any of the `pam_faillock` lines exist without `{include if "with-faillock"}`, run the following command to update the files in `/etc/pam.d` to include `pam_faillock.so`:

```
# authselect apply-changes
```

## References:

1. faillock(8) - Linux man page
2. pam\_faillock(8) - Linux man page
3. NIST SP 800-53 :: AC-7 a
4. NIST SP 800-53A :: AC-7.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-244533  
RULE ID: SV-244533r743848  
STIG ID: RHEL-08-020025  
SEVERITY: CAT II

GROUP ID: V-244534  
RULE ID: SV-244534r743851  
STIG ID: RHEL-08-020026  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                      | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>6.2 <u>Establish an Access Revoking Process</u></b><br>Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. |  |  |  |
| v7               | <b>16.7 <u>Establish Process for Revoking Access</u></b><br>Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.                |                                                                                       |  |  |

### 5.3.2.3 Ensure pam\_pwquality module is enabled (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The **pam\_pwquality.so** module performs password quality checking. This module can be plugged into the password stack of a given service to provide strength-checking for passwords. The code was originally based on pam\_cracklib module and the module is backwards compatible with its options.

The action of this module is to prompt the user for a password and check its strength against a system dictionary and a set of rules for identifying poor choices.

The first action is to prompt for a single password, check its strength and then, if it is considered strong, prompt for the password a second time (to verify that it was typed correctly on the first occasion). All being well, the password is passed on to subsequent modules to be installed as the new authentication token.

#### Rationale:

Use of a unique, complex passwords helps to increase the time and resources required to compromise the password.

#### Audit:

Run the following commands to verify that **pam\_pwquality** is enabled:

```
# grep -P -- '\bpam_pwquality\.so\b' /etc/pam.d/{password,system}-auth
```

Output should be similar to:

```
/etc/pam.d/password-auth:password    requisite    pam_pwquality.so
local_users_only
/etc/pam.d/system-auth:password    requisite    pam_pwquality.so
local_users_only
```

## Remediation:

Review the authselect profile templates:

Run the following script to verify the **pam\_pwquality.so** lines exist in the active profile templates:

```
#!/usr/bin/env bash

{
  l_module_name="pwquality"
  l_pam_profile="$(head -1 /etc/authselect/authselect.conf) "
  if grep -Pq -- '^custom\/' <<< "$l_pam_profile"; then
    l_pam_profile_path="/etc/authselect/$l_pam_profile"
  else
    l_pam_profile_path="/usr/share/authselect/default/$l_pam_profile"
  fi
  grep -P -- "\bpam $l_module_name\.so\b"
  "$l_pam_profile_path"/{password,system}-auth
}
```

*Example Output with a custom profile named "custom-profile":*

```
/etc/authselect/custom/custom-profile/password-auth:password    requisite
pam_pwquality.so local_users_only {include if "with-pwquality"}

/etc/authselect/custom/custom-profile/system-auth:password    requisite
pam_pwquality.so local_users_only {include if "with-pwquality"}
```

**Note:** The lines may not include **{include if "with-pwquality"}**

- **IF** - the lines shown above are not returned, refer to the Recommendation "Ensure active authselect profile includes pam modules" to update the authselect profile template files to include the **pam\_pwquality** entries before continuing this remediation.

- **IF** - any of the **pam\_pwquality** lines include **{include if "with-pwquality"}**, run the following command to enable the authselect **with-pwquality** feature and update the files in **/etc/pam.d** to include **pam\_pwquality**:

```
# authselect enable-feature with-pwquality
```

- **IF** - any of the **pam\_pwquality** lines exist without **{include if "with-pwquality"}**, run the following command to update the files in **/etc/pam.d** to include **pam\_pwquality.so**:

```
# authselect apply-changes
```

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230356  
RULE ID: SV-230356r902728  
STIG ID: RHEL-08-020100  
SEVERITY: CAT II

GROUP ID: V-251713  
RULE ID: SV-251713r902740  
STIG ID: RHEL-08-020101  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |    |    |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques                                                        | Tactics | Mitigations |
|------------------------------------------------------------------------------------|---------|-------------|
| T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004 | TA0006  | M1027       |



### 5.3.2.4 Ensure pam\_pwhistory module is enabled (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The **pam\_history.so** module saves the last passwords for each user in order to force password change history and keep the user from alternating between the same password too frequently.

#### Rationale:

Requiring users not to reuse their passwords make it less likely that an attacker will be able to guess the password or use a compromised password.

#### Audit:

Run the following commands to verify that **pam\_pwhistory** is enabled:

```
# grep -P -- '\bpam_pwhistory\.so\b' /etc/pam.d/{password,system}-auth
```

Output should be similar to:

```
/etc/pam.d/password-auth:password    required    pam_pwhistory.so use_authtok
/etc/pam.d/system-auth:password      required    pam_pwhistory.so use_authtok
```

## Remediation:

Run the following script to verify the **pam\_pwhistory.so** lines exist in the profile templates:

```
#!/usr/bin/env bash

{
  l_module_name="pwhistory"
  l_pam_profile="$(head -1 /etc/authselect/authselect.conf)"
  if grep -Pq -- '^custom\/' <<< "$l_pam_profile"; then
    l_pam_profile_path="/etc/authselect/$l_pam_profile"
  else
    l_pam_profile_path="/usr/share/authselect/default/$l_pam_profile"
  fi
  grep -P -- "\bpam_$l_module_name\.so\b"
  "$l_pam_profile_path"/{password,system}-auth
}
```

*Example Output with a custom profile named "custom-profile":*

```
/etc/authselect/custom/custom-profile/password-auth:password    required
pam_pwhistory.so use_authok {include if "with-pwhistory"}

/etc/authselect/custom/custom-profile/system-auth:password    required
pam_pwhistory.so use_authok {include if "with-pwhistory"}
```

**Note:** The lines may not include **{include if "with-pwhistory"}**

- **IF** - the lines shown above are not returned, refer to the Recommendation "Ensure active authselect profile includes pam modules" to update the authselect profile template files to include the **pam\_pwhistory** entries before continuing this remediation.
- **IF** - the lines include **{include if "with-pwhistory"}**, run the following command to enable the authselect **with-pwhistory** feature and update the files in **/etc/pam.d** to include **pam\_faillock.so**:

```
# authselect enable-feature with-pwhistory
```

- **IF** - any of the **pam\_pwhistory** lines exist without **{include if "with-pwhistory"}**, run the following command to update the files in **/etc/pam.d** to include **pam\_pwhistory.so**:

```
# authselect apply-changes
```

## References:

1. NIST SP 800-53 Rev. 5: IA-5(1)

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques                                                        | Tactics | Mitigations |
|------------------------------------------------------------------------------------|---------|-------------|
| T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004 | TA0006  | M1027       |

### 5.3.2.5 Ensure pam\_unix module is enabled (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The **pam\_unix.so** module is the standard Unix authentication module. It uses standard calls from the system's libraries to retrieve and set account information as well as authentication. Usually this is obtained from the **/etc/passwd** and the **/etc/shadow** file as well if shadow is enabled.

#### Rationale:

Requiring users to use authentication make it less likely that an attacker will be able to access the system.

#### Audit:

Run the following commands to verify that **pam\_unix** is enabled:

```
# grep -P -- '\bpam_unix\.so\b' /etc/pam.d/{password,system}-auth
```

Output should be similar to:

```
/etc/pam.d/password-auth:auth    sufficient    pam_unix.so
/etc/pam.d/password-auth:account  required     pam_unix.so
/etc/pam.d/password-auth:password sufficient    pam_unix.so sha512 shadow
use_authok
/etc/pam.d/password-auth:session  required     pam_unix.so

/etc/pam.d/system-auth:auth    sufficient    pam_unix.so
/etc/pam.d/system-auth:account  required     pam_unix.so
/etc/pam.d/system-auth:password sufficient    pam_unix.so sha512 shadow
use_authok
/etc/pam.d/system-auth:session  required     pam_unix.so
```

## Remediation:

Run the following script to verify the **pam\_unix.so** lines exist in the profile templates:

```
#!/usr/bin/env bash

{
  l_module_name="unix"
  l_pam_profile="$(head -1 /etc/authselect/authselect.conf) "
  if grep -Pq -- '^custom\/' <<< "$l_pam_profile"; then
    l_pam_profile_path="/etc/authselect/$l_pam_profile"
  else
    l_pam_profile_path="/usr/share/authselect/default/$l_pam_profile"
  fi
  grep -P -- "\bpam_$l_module_name\.so\b"
  "$l_pam_profile_path"/{password,system}-auth
}
```

*Example Output with a custom profile named "custom-profile":*

```
/etc/authselect/custom/custom-profile/password-auth:auth    sufficient
pam_unix.so {if not "without-nullok":nullok}
/etc/authselect/custom/custom-profile/password-auth:account  required
pam_unix.so
/etc/authselect/custom/custom-profile/password-auth:password  sufficient
pam_unix.so sha512 shadow {if not "without-nullok":nullok} use_authtok
remember=5
/etc/authselect/custom/custom-profile/password-auth:session  required
pam_unix.so

/etc/authselect/custom/custom-profile/system-auth:auth    sufficient
pam_unix.so {if not "without-nullok":nullok}
/etc/authselect/custom/custom-profile/system-auth:account  required
pam_unix.so
/etc/authselect/custom/custom-profile/system-auth:password  sufficient
pam_unix.so sha512 shadow {if not "without-nullok":nullok} use_authtok
/etc/authselect/custom/custom-profile/system-auth:session  required
pam_unix.so
```

- **IF** - the lines shown above are not returned, refer to the Recommendation "Ensure active authselect profile includes pam modules" to update the authselect profile template files to include the **pam\_unix** entries before continuing this remediation.

**Note:** Arguments following **pam\_unix.so** may be different than the example output

## References:

1. NIST SP 800-53 Rev. 5: IA-5(1)

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                                                        | Tactics | Mitigations |
|------------------------------------------------------------------------------------|---------|-------------|
| T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004 | TA0006  | M1027       |

### 5.3.3 Configure PAM Arguments

Pluggable Authentication Modules (PAM) uses arguments to pass information to a pluggable module during authentication for a particular module type. These arguments allow the PAM configuration files for particular programs to use a common PAM module but in different ways.

Invalid arguments are ignored and do not otherwise affect the success or failure of the PAM module. When an invalid argument is passed, an error is usually written to `/var/log/messages` file. However, since the reporting method is controlled by the PAM module, the module must be written correctly to log the error to this file.

### 5.3.3.1 Configure pam\_faillock module

faillock.conf provides a way to configure the default settings for locking the user after multiple failed authentication attempts. This file is read by the pam\_faillock module and is the preferred method over configuring pam\_faillock directly.

The file has a very simple name = value format with possible comments starting with # character. The whitespace at the beginning of line, end of line, and around the = sign is ignored.

Options:

- **<dir=/path/to/tally-directory>** - The directory where the user files with the failure records are kept. The default is /var/run/faillock. Note: These files will disappear after reboot on systems configured with directory /var/run/faillock mounted on virtual memory.
- **audit** - Will log the user name into the system log if the user is not found.
- **silent** - Don't print informative messages to the user. Please note that when this option is not used there will be difference in the authentication behavior for users which exist on the system and non-existing users.
- **no\_log\_info** - Don't log informative messages via syslog(3).
- **local\_users\_only** - Only track failed user authentications attempts for local users in /etc/passwd and ignore centralized (AD, IdM, LDAP, etc.) users. The faillock(8) command will also no longer track user failed authentication attempts. Enabling this option will prevent a double-lockout scenario where a user is locked out locally and in the centralized mechanism.
- **nodelay** - Don't enforce a delay after authentication failures.
- **deny=<n>** - Deny access if the number of consecutive authentication failures for this user during the recent interval exceeds . The default is 3.
- **fail\_interval=n** - The length of the interval during which the consecutive authentication failures must happen for the user account lock out is n seconds. The default is 900 (15 minutes).
- **unlock\_time=n** - The access will be re-enabled after n seconds after the lock out. The value 0 has the same meaning as value never - the access will not be re-enabled without resetting the faillock entries by the faillock(8) command. The default is 600 (10 minutes). Note that the default directory that pam\_faillock uses is usually cleared on system boot so the access will be also re-enabled after system reboot. If that is undesirable a different tally directory must be set with the dir option. Also note that it is usually undesirable to permanently lock out users as they can become easily a target of denial of service attack unless the usernames are random and kept secret to potential attackers.
- **even\_deny\_root** - Root account can become locked as well as regular accounts.
- **root\_unlock\_time=n** - This option implies even\_deny\_root option. Allow access after n seconds to root account after the account is locked. In case the option is not specified the value is the same as of the unlock\_time option.
- **admin\_group=name** - If a group name is specified with this option, members of the group will be handled by this module the same as the root account (the



options `even_deny_root` and `root_unlock_time` will apply to them. By default the option is not set.

*Example `/etc/security/faillock.conf` file:*

```
deny=5
unlock_time=900
even_deny_root
```

### 5.3.3.1.1 Ensure password failed attempts lockout is configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The **deny=<n>** option will deny access if the number of consecutive authentication failures for this user during the recent interval exceeds .

#### Rationale:

Locking out user IDs after *n* unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

#### Audit:

Run the following command to verify that Number of failed logon attempts before the account is locked is no greater than **5** and meets local site policy:

```
# grep -Pi -- '^\\h*deny\\h*=\\h*[1-5]\\b' /etc/security/faillock.conf
deny = 5
```

Run the following command to verify that the **deny** argument has not been set, or is set to 5 or less and meets local site policy:

```
# grep -Pi --
'^\\h*auth\\h+(requisite|required|sufficient)\\h+pam_faillock\\.so\\h+([^\n\r]+\h
+)?deny\\h*=\\h*(0|[6-9]|[1-9][0-9]+)\\b' /etc/pam.d/system-auth
/etc/pam.d/password-auth
Nothing should be returned
```

## Remediation:

Create or edit the following line in `/etc/security/faillock.conf` setting the `deny` option to **5** or less:

```
deny = 5
```

Run the following script to remove the `deny` argument from the `pam_faillock.so` module in the PAM files:

```
#!/usr/bin/env bash
{
  for l_pam_file in system-auth password-auth; do
    l_authselect_file="/etc/authselect/${head -1
/etc/authselect/authselect.conf | grep 'custom/'}/$l_pam_file"
    sed -ri
's/(^\s*auth\s+(requisite|required|sufficient)\s+pam_faillock\.so.*) (\s+deny\s
s*=\s*\S+) (.*)/\1\4/' "$l_authselect_file"
  done
  authselect apply-changes
}
```

## Default Value:

`deny = 3`

## Additional Information:

If a user has been locked out because they have reached the maximum consecutive failure count defined by `deny=` in the `pam_faillock.so` module, the user can be unlocked by issuing the command `faillock --user <USERNAME> --reset`. This command sets the failed count to 0, effectively unlocking the user.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>6.2 Establish an Access Revoking Process</b><br>Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. |  |  |  |
| v7               | <b>16.7 Establish Process for Revoking Access</b><br>Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.                 |                                                                                       |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1110, T1110.001, T1110.003 | TA0006  | M1027       |

### 5.3.3.1.2 Ensure password unlock time is configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

`unlock_time=<n>` - The access will be re-enabled after seconds after the lock out. The value `0` has the same meaning as value never - the access will not be re-enabled without resetting the faillock entries by the `faillock(8)` command.

#### Notes:

- The default directory that `pam_faillock` uses is usually cleared on system boot so the access will be also re-enabled after system reboot. If that is undesirable a different tally directory must be set with the `dir` option.
- It is usually undesirable to permanently lock out users as they can become easily a target of denial of service attack unless the usernames are random and kept secret to potential attackers.
- The maximum configurable value for `unlock_time` is `604800`

#### Rationale:

Locking out user IDs after *n* unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

#### Impact:

Use of `unlock_time=0` may allow an attacker to cause denial of service to legitimate users. This will also require a systems administrator with elevated privileges to unlock the account.

## Audit:

Run the following command to verify that the time in seconds before the account is unlocked is either 0 (never) or 900 (15 minutes) or more and meets local site policy:

```
# grep -Pi -- '^h*unlock_timeh*=\h*(0|9[0-9][0-9]|[1-9][0-9]{3,})\b'
/etc/security/faillock.conf

unlock_time = 900
```

Run the following command to verify that the `unlock_time` argument has not been set, or is either 0 (never) or 900 (15 minutes) or more and meets local site policy:

```
# grep -Pi --
'^h*authh+(requisite|required|sufficient)\h+pam_faillock\.so\h+([\#\n\r]+\h
+)?unlock_timeh*=\h*([1-9]|[1-9][0-9]|[1-8][0-9][0-9])\b' /etc/pam.d/system-
auth /etc/pam.d/password-auth

Nothing should be returned
```

## Remediation:

Set password unlock time to conform to site policy. `unlock_time` should be 0 (never), or 900 seconds or greater.

Edit `/etc/security/faillock.conf` and update or add the following line:

```
unlock_time = 900
```

Run the following script to remove the `unlock_time` argument from the `pam_faillock.so` module in the PAM files:

```
#!/usr/bin/env bash
{
    for l_pam_file in system-auth password-auth; do
        l_authselect_file="/etc/authselect/${head -1
/etc/authselect/authselect.conf | grep 'custom/'}/$l_pam_file"
        sed -ri
        's/(\^s*auth\s+(requisite|required|sufficient)\s+pam_faillock\.so.*) (\s+unloc
k_time\s*=\s*\S+) (.*)/\1\4/' "$l_authselect_file"
        done
        authselect apply-changes
    }
}
```

## Default Value:

```
unlock_time = 600
```

## Additional Information:

If a user has been locked out because they have reached the maximum consecutive failure count defined by `deny=` in the `pam_faillock.so` module, the user can be unlocked by issuing the command `faillock --user <USERNAME> --reset`. This command sets the failed count to 0, effectively unlocking the user.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                      | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>6.2 <u>Establish an Access Revoking Process</u></b><br>Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. | ●    | ●    | ●    |
| v7               | <b>16.7 <u>Establish Process for Revoking Access</u></b><br>Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.                |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1110, T1110.001, T1110.003 | TA0006  | M1027       |

### 5.3.3.1.3 *Ensure password failed attempts lockout includes root account (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

`even_deny_root` - Root account can become locked as well as regular accounts

`root_unlock_time=n` - This option implies `even_deny_root` option. Allow access after n seconds to root account after the account is locked. In case the option is not specified the value is the same as of the `unlock_time` option.

#### **Rationale:**

Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

#### **Impact:**

Use of `unlock_time=0` or `root_unlock_time=0` may allow an attacker to cause denial of service to legitimate users.



## Audit:

Run the following command to verify that **even\_deny\_root** and/or **root\_unlock\_time** is enabled:

```
# grep -Pi -- '^\\h*(even_deny_root|root_unlock_time\\h*=\\h*\\d+)\\b' /etc/security/faillock.conf
```

*Example output:*

```
even_deny_root
--AND/OR--
root_unlock_time = 60
```

Run the following command to verify that - **IF** - **root\_unlock\_time** is set, it is set to **60** (One minute) or more:

```
# grep -Pi -- '^\\h*root_unlock_time\\h*=\\h*([1-9]|[1-5][0-9])\\b' /etc/security/faillock.conf
```

Nothing should be returned

Run the following command to check the **pam\_faillock.so** module for the **root\_unlock\_time** argument. Verify - **IF** - **root\_unlock\_time** is set, it is set to **60** (One minute) or more:

```
# grep -Pi -- '^\\h*auth\\h+([\\^#\\n\\r]+\\h+)pam_faillock\\.so\\h+([\\^#\\n\\r]+\\h+)?root_unlock_time\\h*=\\h*([1-9]|[1-5][0-9])\\b' /etc/pam.d/system-auth /etc/pam.d/password-auth
```

Nothing should be returned

## Remediation:

Edit `/etc/security/faillock.conf`:

- Remove or update any line containing `root_unlock_time`, - **OR** - set it to a value of `60` or more
- Update or add the following line:

```
even_deny_root
```

Run the following script to remove the `even_deny_root` and `root_unlock_time` arguments from the `pam_faillock.so` module in the PAM files:

```
#!/usr/bin/env bash
{
    for l_pam_file in system-auth password-auth; do
        l_authselect_file="/etc/authselect/${head -1
/etc/authselect/authselect.conf | grep 'custom/'}/$l_pam_file"
        sed -ri
's/(\s*auth\s+(.*)\s+pam_faillock\.so.*) (\s+even_deny_root) (.*)/\1\4/'
"$l_authselect_file"
        sed -ri
's/(\s*auth\s+(.*)\s+pam_faillock\.so.*) (\s+root_unlock_time\s*=\s*\S+) (.*)
/\1\4/' "$l_authselect_file"
    done
    authselect apply-changes
}
\`
```

## Default Value:

disabled

## Additional Information:

If a user has been locked out because they have reached the maximum consecutive failure count defined by `deny=` in the `pam_faillock.so` module, the user can be unlocked by issuing the command `faillock --user <USERNAME> --reset`. This command sets the failed count to 0, effectively unlocking the user.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                      | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>6.2 <u>Establish an Access Revoking Process</u></b><br>Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. | ●    | ●    | ●    |
| v7               | <b>16.7 <u>Establish Process for Revoking Access</u></b><br>Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.                |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1110, T1110.001, T1110.003 | TA0006  | M1027       |

### *5.3.3.1.4 Ensure deny is configured on the pam\_faillock module (Automated)*

**Profile Applicability:**

- STIG

**Description:**

The operating system must automatically lock an account when three unsuccessful logon attempts occur.

**Rationale:**

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

RHEL 8 operating systems can utilize the "pam\_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program.

From "Pam\_Faillock" man pages: Note that the default directory that "pam\_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

## Audit:

Check that the system locks an account after three unsuccessful logon attempts with the following commands:

### Note:

- If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.
- This check applies to RHEL versions 8.0 and 8.1, if the system is RHEL version 8.2 or newer, this check is not applicable.

```
# grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "deny" option is not set to "3" or less (but not "0") on the "preauth" line with the "pam\_faillock.so" module, or is missing from this line, this is a finding.

If any line referencing the "pam\_faillock.so" module is commented out, this is a finding.

```
# grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "deny" option is not set to "3" or less (but not "0") on the "preauth" line with the "pam\_faillock.so" module, or is missing from this line, this is a finding.

If any line referencing the "pam\_faillock.so" module is commented out, this is a finding.

## Remediation:

Configure the operating system to lock an account when three unsuccessful logon attempts occur.

Add/Modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
# systemctl restart sssd.service
```

## References:

1. NIST SP 800-53 :: AC-7 a
2. NIST SP 800-53A :: AC-7.1 (ii)

## Additional Information:

```
Red Hat Enterprise Linux 8
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230332
RULE ID: SV-230332r627750
STIG ID: RHEL-08-020010
SEVERITY: CAT II
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>6.2 Establish an Access Revoking Process</b><br>Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. |  |  |  |
| v7               | <b>16.7 Establish Process for Revoking Access</b><br>Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.                |                                                                                       |  |  |

### 5.3.3.1.5 Ensure deny is configured in /etc/security/faillock.conf (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must automatically lock an account when three unsuccessful logon attempts occur.

#### Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In RHEL 8.2 the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the pam\_faillock.so module. Also introduced is a "local\_users\_only" option that will only track failed user authentication attempts for local users in /etc/passwd and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam\_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

#### Audit:

**Note:** This check applies to RHEL versions 8.2 or newer, if the system is RHEL version 8.0 or 8.1, this check is not applicable.

Verify the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts:

```
# grep 'deny =' /etc/security/faillock.conf  
deny = 3
```

If the "deny" option is not set to "3" or less (but not "0"), is missing or commented out, this is a finding.

## Remediation:

Configure the operating system to lock an account when three unsuccessful logon attempts occur.

Add/Modify the "/etc/security/faillock.conf" file to match the following line:

```
deny = 3
```

## References:

1. NIST SP 800-53 :: AC-7 a
2. NIST SP 800-53A :: AC-7.1 (ii)

## Additional Information:

```
Red Hat Enterprise Linux 8
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230333
RULE ID: SV-230333r743966
STIG ID: RHEL-08-020011
SEVERITY: CAT II
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                      | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>6.2 <u>Establish an Access Revoking Process</u></b><br>Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. |  |  |  |
| v7               | <b>16.7 <u>Establish Process for Revoking Access</u></b><br>Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.                |                                                                                       |  |  |



### *5.3.3.1.6 Ensure fail\_interval is configured on the pam\_faillock module (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.

#### **Rationale:**

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

RHEL 8 operating systems can utilize the "pam\_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program.

From "Pam\_Faillock" man pages: Note that the default directory that "pam\_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

## Audit:

Check that the system locks an account after three unsuccessful logon attempts within a period of 15 minutes with the following commands:

### Note:

- If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.
- This check applies to RHEL versions 8.0 and 8.1, if the system is RHEL version 8.2 or newer, this check is not applicable.

```
# grep pam_faillock.so /etc/pam.d/password-auth
```

### Output:

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "fail\_interval" option is not set to **900** or less (but not **0**) on the **preauth** lines with the **pam\_faillock.so** module, or is missing from this line, this is a finding.

```
# grep pam_faillock.so /etc/pam.d/system-auth
```

### Output:

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "fail\_interval" option is not set to **900** or less (but not **0**) on the **preauth** lines with the **pam\_faillock.so** module, or is missing from this line, this is a finding

## Remediation:

Configure the operating system to lock an account until released by an administrator when three unsuccessful logon attempts occur in 15 minutes.

Add/Modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
# systemctl restart sssd.service
```

## References:

1. NIST SP 800-53 :: AC-7 a
2. NIST SP 800-53A :: AC-7.1 (ii)

## Additional Information:

```
Red Hat Enterprise Linux 8
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230334
RULE ID: SV-230334r627750
STIG ID: RHEL-08-020012
SEVERITY: CAT II
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>6.2 Establish an Access Revoking Process</b><br>Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. |  |  |  |
| v7               | <b>16.7 Establish Process for Revoking Access</b><br>Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.                |                                                                                       |  |  |

### 5.3.3.1.7 Ensure fail\_interval is configured in /etc/security/faillock.conf (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must automatically lock an account when three unsuccessful logon attempts occur during a 15-minute time period.

#### Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In RHEL 8.2 operating systems the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the pam\_faillock.so module. Also introduced is a "local\_users\_only" option that will only track failed user authentication attempts for local users in "/etc/passwd" and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam\_faillock" uses is usually cleared on system boot so the access will be re-enabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

#### Audit:

**Note:** This check applies to RHEL versions 8.2 or newer, if the system is RHEL version 8.0 or 8.1, this check is not applicable.

Verify the "/etc/security/faillock.conf" file is configured to lock an account after three unsuccessful logon attempts within 15 minutes:

```
# grep 'fail_interval =' /etc/security/faillock.conf  
fail_interval = 900
```

If the "fail\_interval" option is not set to "900" or more, is missing or commented out, this is a finding.

## Remediation:

Configure the operating system to lock an account when three unsuccessful logon attempts occur in 15 minutes.

Add/Modify the "/etc/security/faillock.conf" file to match the following line:

```
fail_interval = 900
```

## References:

1. NIST SP 800-53 :: AC-7 a
2. NIST SP 800-53A :: AC-7.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230335  
RULE ID: SV-230335r743969  
STIG ID: RHEL-08-020013  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>6.2 Establish an Access Revoking Process</b><br>Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. |  |  |  |
| v7               | <b>16.7 Establish Process for Revoking Access</b><br>Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.                |                                                                                       |  |  |

### *5.3.3.1.8 Ensure unlock\_time is configured on the pam\_faillock module (Automated)*

**Profile Applicability:**

- STIG

**Description:**

The operating system must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.

**Rationale:**

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

RHEL 8 operating systems can utilize the "pam\_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program.

From "Pam\_Faillock" man pages: Note that the default directory that "pam\_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

## Audit:

Check that the system locks an account after three unsuccessful logon attempts within a period of 15 minutes until released by an administrator with the following commands:

### Note:

- If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.
- This check applies to RHEL versions 8.0 and 8.1, if the system is RHEL version 8.2 or newer, this check is not applicable.

```
# grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "unlock\_time" option is not set to "0" on the "preauth" and "authfail" lines with the "pam\_faillock.so" module, or is missing from these lines, this is a finding.

```
# grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "unlock\_time" option is not set to "0" on the "preauth" and "authfail" lines with the "pam\_faillock.so" module, or is missing from these lines, this is a finding.

## Remediation:

Configure the operating system to lock an account until released by an administrator when three unsuccessful logon attempts occur in 15 minutes.

Add/Modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
# systemctl restart sssd.service
```

## References:

1. NIST SP 800-53 :: AC-7 a
2. NIST SP 800-53A :: AC-7.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230336  
RULE ID: SV-230336r627750  
STIG ID: RHEL-08-020014  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                      | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>6.2 <u>Establish an Access Revoking Process</u></b><br>Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. |  |  |  |
| v7               | <b>16.7 <u>Establish Process for Revoking Access</u></b><br>Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.                |                                                                                     |  |  |



### 5.3.3.1.9 Ensure unlock\_time is configured in /etc/security/faillock.conf (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.

#### Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In RHEL 8.2 operating systems the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the pam\_faillock.so module. Also introduced is a "local\_users\_only" option that will only track failed user authentication attempts for local users in /etc/passwd and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam\_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

#### Audit:

**Note:** This check applies to RHEL versions 8.2 or newer, if the system is RHEL version 8.0 or 8.1, this check is not applicable.

Verify the "/etc/security/faillock.conf" file is configured to lock an account until released by an administrator after three unsuccessful logon attempts:

```
# grep 'unlock_time =' /etc/security/faillock.conf  
unlock_time = 0
```

If the "unlock\_time" option is not set to "0", is missing or commented out, this is a finding.

## Remediation:

Configure the operating system to lock an account until released by an administrator when three unsuccessful logon attempts occur in 15 minutes.

Add/Modify the "/etc/security/faillock.conf" file to match the following line:

```
unlock_time = 0
```

## References:

1. NIST SP 800-53 :: AC-7 a
2. NIST SP 800-53A :: AC-7.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230337  
RULE ID: SV-230337r743972  
STIG ID: RHEL-08-020015  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>6.2 Establish an Access Revoking Process</b><br>Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. |  |  |  |
| v7               | <b>16.7 Establish Process for Revoking Access</b><br>Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.                |                                                                                       |  |  |

### *5.3.3.1.10 Ensure dir is configured on the pam\_faillock module (Automated)*

**Profile Applicability:**

- STIG

**Description:**

The operating system must ensure account lockouts persist.

**Rationale:**

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

RHEL 8 operating systems can utilize the "pam\_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program.

From "Pam\_Faillock" man pages: Note that the default directory that "pam\_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

## Audit:

Check that the faillock directory contents persists after a reboot with the following commands:

### Note:

- If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.
- This check applies to RHEL versions 8.0 and 8.1, if the system is RHEL version 8.2 or newer, this check is not applicable.

```
# grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "dir" option is not set to a non-default documented tally log directory on the "preauth" and "authfail" lines with the "pam\_faillock.so" module, or is missing from these lines, this is a finding.

```
# grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "dir" option is not set to a non-default documented tally log directory on the "preauth" and "authfail" lines with the "pam\_faillock.so" module, or is missing from these lines, this is a finding.

## Remediation:

Configure the operating system maintain the contents of the faillock directory after a reboot.

Add/Modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

**Note:** Using the default faillock directory of /var/run/faillock will result in the contents being cleared in the event of a reboot.

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
# systemctl restart sssd.service
```

## References:

1. NIST SP 800-53 :: AC-7 a
2. NIST SP 800-53A :: AC-7.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230338  
RULE ID: SV-230338r627750  
STIG ID: RHEL-08-020016  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>6.2 Establish an Access Revoking Process</b><br>Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. |  |  |  |
| v7               | <b>16.7 Establish Process for Revoking Access</b><br>Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.                |                                                                                       |  |  |

### 5.3.3.1.11 Ensure dir is configured in /etc/security/faillock.conf (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must ensure account lockouts persist.

#### Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In RHEL 8.2 operating systems the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the pam\_faillock.so module. Also introduced is a "local\_users\_only" option that will only track failed user authentication attempts for local users in /etc/passwd and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From "faillock.conf" man pages: Note that the default directory that "pam\_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

#### Audit:

**Note:** This check applies to RHEL versions 8.2 or newer. If the system is RHEL version 8.0 or 8.1, this check is not applicable.

Verify the "/etc/security/faillock.conf" file is configured use a non-default faillock directory to ensure contents persist after reboot:

```
# grep 'dir =' /etc/security/faillock.conf  
  
dir = /var/log/faillock
```

If the "dir" option is not set to a non-default documented tally log directory, is missing or commented out, this is a finding.

## Remediation:

Configure the operating system maintains the contents of the faillock directory after a reboot.

Add/Modify the "/etc/security/faillock.conf" file to match the following line:

```
dir = /var/log/faillock
```

## References:

1. NIST SP 800-53 :: AC-7 a
2. NIST SP 800-53A :: AC-7.1 (ii)

## Additional Information:

```
Red Hat Enterprise Linux 8
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230339
RULE ID: SV-230339r743975
STIG ID: RHEL-08-020017
SEVERITY: CAT II
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                      | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>6.2 <u>Establish an Access Revoking Process</u></b><br>Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. |  |  |  |
| v7               | <b>16.7 <u>Establish Process for Revoking Access</u></b><br>Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.                |                                                                                       |  |  |

### *5.3.3.1.12 Ensure silent is set on the pam\_faillock module (Automated)*

**Profile Applicability:**

- STIG

**Description:**

The operating system must prevent system messages from being presented when three unsuccessful logon attempts occur.

**Rationale:**

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

RHEL 8 operating systems can utilize the "pam\_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program.

From "Pam\_Faillock" man pages: Note that the default directory that "pam\_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128



## Audit:

Check that the system prevents informative messages from being presented to the user pertaining to logon information with the following commands:

### Note:

- If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.
- This check applies to RHEL versions 8.0 and 8.1, if the system is RHEL version 8.2 or newer, this check is not applicable.

```
# grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "silent" option is missing from the "preauth" line with the "pam\_faillock.so" module, this is a finding.

```
# grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "silent" option is missing from the "preauth" line with the "pam\_faillock.so" module, this is a finding.

## Remediation:

Configure the operating system to prevent informative messages from being presented at logon attempts.

Add/Modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
# systemctl restart sssd.service
```

## References:

1. NIST SP 800-53 :: AC-7 a
2. NIST SP 800-53A :: AC-7.1 (ii)

### Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230340  
RULE ID: SV-230340r627750  
STIG ID: RHEL-08-020018  
SEVERITY: CAT II

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### 5.3.3.1.13 Ensure silent is set in /etc/security/faillock.conf (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must prevent system messages from being presented when three unsuccessful logon attempts occur.

#### Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In RHEL 8.2 operating systems the `/etc/security/faillock.conf` file was incorporated to centralize the configuration of the `pam_faillock.so` module. Also introduced is a `"local_users_only"` option that will only track failed user authentication attempts for local users in `/etc/passwd` and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From `"faillock.conf"` man pages: Note that the default directory that `"pam_faillock"` uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the `"dir"` option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

#### Audit:

**Note:** This check applies to RHEL versions 8.2 or newer, if the system is RHEL version 8.0 or 8.1, this check is not applicable.

Verify the `/etc/security/faillock.conf` file is configured to prevent informative messages from being presented at logon attempts:

```
# grep silent /etc/security/faillock.conf
silent
```

If the `"silent"` option is not set, is missing or commented out, this is a finding.

## Remediation:

Configure the operating system to prevent informative messages from being presented at logon attempts.

Add/Modify the "/etc/security/faillock.conf" file to match the following line:

```
silent
```

## References:

1. NIST SP 800-53 :: AC-7 a
2. NIST SP 800-53A :: AC-7.1 (ii)

## Additional Information:

```
Red Hat Enterprise Linux 8
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230341
RULE ID: SV-230341r743978
STIG ID: RHEL-08-020019
SEVERITY: CAT II
```

## CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### *5.3.3.1.14 Ensure audit is set on the pam\_faillock module (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must log user name information when unsuccessful logon attempts occur.

#### **Rationale:**

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

RHEL 8 operating systems can utilize the "pam\_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program.

From "Pam\_Faillock" man pages: Note that the default directory that "pam\_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

The "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the "pam\_faillock.so" module. Also introduced is a "local\_users\_only" option that will only track failed user authentication attempts for local users in "/etc/passwd" and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

## Audit:

Check that the system logs user name information when unsuccessful logon attempts occur with the following commands:

### Note:

- If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.
- If the system is RHEL version 8.2 or newer, this check is not applicable.

```
# grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "audit" option is missing from the "preauth" line with the "pam\_faillock.so" module, this is a finding.

```
# grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "audit" option is missing from the "preauth" line with the "pam\_faillock.so" module, this is a finding.

## Remediation:

Configure the operating system to log user name information when unsuccessful logon attempts occur.

Add/Modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
# systemctl restart sssd.service
```

## References:

1. NIST SP 800-53 :: AC-7 a
2. NIST SP 800-53A :: AC-7.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230342  
RULE ID: SV-230342r646872  
STIG ID: RHEL-08-020020  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      |  |  |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.                                                                                |      |  |  |

### 5.3.3.1.15 Ensure audit is set in /etc/security/faillock.conf (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must log user name information when unsuccessful logon attempts occur.

#### Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In RHEL 8.2 operating systems the `/etc/security/faillock.conf` file was incorporated to centralize the configuration of the `pam_faillock.so` module. Also introduced is a `"local_users_only"` option that will only track failed user authentication attempts for local users in `/etc/passwd` and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From `"faillock.conf"` man pages: Note that the default directory that `"pam_faillock"` uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the `"dir"` option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

#### Audit:

**Note:** This check applies to RHEL versions 8.2 or newer, if the system is RHEL version 8.0 or 8.1, this check is not applicable.

Verify the `/etc/security/faillock.conf` file is configured to log user name information when unsuccessful logon attempts occur:

```
# grep audit /etc/security/faillock.conf  
audit
```

If the `"audit"` option is not set, is missing or commented out, this is a finding.



## Remediation:

Configure the operating system to log user name information when unsuccessful logon attempts occur.

Add/Modify the "/etc/security/faillock.conf" file to match the following line:

```
audit
```

## References:

1. NIST SP 800-53 :: AC-7 a
2. NIST SP 800-53A :: AC-7.1 (ii)

## Additional Information:

```
Red Hat Enterprise Linux 8
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230343
RULE ID: SV-230343r743981
STIG ID: RHEL-08-020021
SEVERITY: CAT II
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.                                                                                |      | ●    | ●    |

### *5.3.3.1.16 Ensure even\_deny\_root is set on the pam\_faillock module (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must include root when automatically locking an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.

#### **Rationale:**

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

RHEL 8 operating systems can utilize the "pam\_faillock.so" for this purpose. Note that manual changes to the listed files may be overwritten by the "authselect" program.

From "Pam\_Faillock" man pages: Note that the default directory that "pam\_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

The "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the "pam\_faillock.so" module. Also introduced is a "local\_users\_only" option that will only track failed user authentication attempts for local users in "/etc/passwd" and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

## Audit:

Check that the system includes the root account when locking an account after three unsuccessful logon attempts within a period of 15 minutes with the following commands:

### Note:

- If the System Administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is not applicable.
- If the system is RHEL version 8.2 or newer, this check is not applicable.

```
# grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "even\_deny\_root" option is missing from the "preauth" line with the "pam\_faillock.so" module, this is a finding.

```
# grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

If the "even\_deny\_root" option is missing from the "preauth" line with the "pam\_faillock.so" module, this is a finding.

## Remediation:

Configure the operating system to include root when locking an account after three unsuccessful logon attempts occur in 15 minutes.

Add/Modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

```
auth required pam_faillock.so preauth dir=/var/log/faillock silent audit
deny=3 even_deny_root fail_interval=900 unlock_time=0
auth required pam_faillock.so authfail dir=/var/log/faillock unlock_time=0
account required pam_faillock.so
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
# systemctl restart sssd.service
```

## References:

1. NIST SP 800-53 :: AC-7 a
2. NIST SP 800-53A :: AC-7.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230344  
RULE ID: SV-230344r646874  
STIG ID: RHEL-08-020022  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                      | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>6.2 <u>Establish an Access Revoking Process</u></b><br>Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. |  |  |  |
| v7               | <b>16.7 <u>Establish Process for Revoking Access</u></b><br>Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.                |                                                                                     |  |  |

### 5.3.3.1.17 Ensure even\_deny\_root is set in /etc/security/faillock.conf (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must include root when automatically locking an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.

#### Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

In RHEL 8.2 operating systems the "/etc/security/faillock.conf" file was incorporated to centralize the configuration of the pam\_faillock.so module. Also introduced is a "local\_users\_only" option that will only track failed user authentication attempts for local users in /etc/passwd and ignore centralized (AD, IdM, LDAP, etc.) users to allow the centralized platform to solely manage user lockout.

From the "faillock.conf" man pages: Note that the default directory that "pam\_faillock" uses is usually cleared on system boot so the access will be re-enabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000021-GPOS-00005, SRG-OS-000329-GPOS-00128

#### Audit:

**Note:** This check applies to RHEL versions 8.2 or newer, if the system is RHEL version 8.0 or 8.1, this check is not applicable.

Verify the "/etc/security/faillock.conf" file is configured to log user name information when unsuccessful logon attempts occur:

```
# grep even_deny_root /etc/security/faillock.conf
even_deny_root
```

If the "even\_deny\_root" option is not set, is missing or commented out, this is a finding.

## Remediation:

Configure the operating system to include root when locking an account after three unsuccessful logon attempts occur in 15 minutes.

Add/Modify the "/etc/security/faillock.conf" file to match the following line:

```
even_deny_root
```

## References:

1. NIST SP 800-53 :: AC-7 a
2. NIST SP 800-53A :: AC-7.1 (ii)

## Additional Information:

```
Red Hat Enterprise Linux 8
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230345
RULE ID: SV-230345r743984
STIG ID: RHEL-08-020023
SEVERITY: CAT II
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                      | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>6.2 <u>Establish an Access Revoking Process</u></b><br>Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. |  |  |  |
| v7               | <b>16.7 <u>Establish Process for Revoking Access</u></b><br>Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.                |                                                                                       |  |  |

### *5.3.3.1.18 Ensure the use of a non-default faillock tally directory while SELinux enforces a targeted policy (Manual)*

**Profile Applicability:**

- STIG

**Description:**

The Operating System (OS) must configure SELinux context type to allow the use of a non-default faillock tally directory.

**Rationale:**

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

From "faillock.conf" man pages: Note that the default directory that "pam\_faillock" uses is usually cleared on system boot so the access will be re-enabled after system reboot. If that is undesirable, a different tally directory must be set with the "dir" option.

SELinux, enforcing a targeted policy, will require any non-default tally directory's security context type to match the default directory's security context type. Without updating the security context type, the pam\_faillock module will not write failed login attempts to the non-default tally directory.

## Audit:

### Note:

- If the system does not have SELinux enabled and enforcing a targeted policy, or if the pam\_faillock module is not configured for use, this requirement is not applicable.
- This check applies to RHEL versions 8.2 or newer. If the system is RHEL version 8.0 or 8.1, this check is not applicable.

Verify the location of the non-default tally directory for the pam\_faillock module with the following command:

```
# grep -w dir /etc/security/faillock.conf  
  
dir = /var/log/faillock
```

Check the security context type of the non-default tally directory with the following command:

```
# ls -Zd /var/log/faillock  
  
unconfined_u:object_r:faillog_t:s0 /var/log/faillock
```

If the security context type of the non-default tally directory is not "faillog\_t", this is a finding.

### Remediation:

Configure RHEL 8 to allow the use of a non-default faillock tally directory while SELinux enforces a targeted policy.

Create a non-default faillock tally directory (if it does not already exist) with the following example:

```
# mkdir /var/log/faillock
```

Update the `/etc/selinux/targeted/contexts/files/file_contexts.local` with `faillog_t` context type for the non-default faillock tally directory with the following command:

```
# semanage fcontext -a -t faillog_t "/var/log/faillock(/.*)?"
```

Next, update the context type of the non-default faillock directory/subdirectories and files with the following command:

```
# restorecon -R -v /var/log/faillock
```

### References:

1. NIST SP 800-53 :: AC-7 a
2. NIST SP 800-53A :: AC-7.1 (ii)
3. NIST SP 800-53 Revision 5 :: AC-7 b



## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-250315  
RULE ID: SV-250315r854079  
STIG ID: RHEL-08-020027  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                      | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>6.2 <u>Establish an Access Revoking Process</u></b><br>Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. |  |  |  |
| v7               | <b>16.7 <u>Establish Process for Revoking Access</u></b><br>Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.                |                                                                                     |  |  |

### *5.3.3.1.19 Ensure the use of a non-default faillock tally directory on the pam\_faillock module while SELinux enforces a targeted policy (Manual)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The Operating system (OS) must configure SELinux context type to allow the use of a non-default faillock tally directory.

#### **Rationale:**

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

From "Pam\_Faillock" man pages: Note that the default directory that "pam\_faillock" uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable, a different tally directory must be set with the "dir" option.

SELinux, enforcing a targeted policy, will require any non-default tally directory's security context type to match the default directory's security context type. Without updating the security context type, the pam\_faillock module will not write failed login attempts to the non-default tally directory.

**Audit:****Note:**

- If the system does not have SELinux enabled and enforcing a targeted policy, or if the pam\_faillock module is not configured for use, this requirement is not applicable.
- This check applies to RHEL versions 8.0 and 8.1. If the system is RHEL version 8.2 or newer, this check is not applicable.

Verify the location of the non-default tally directory for the pam\_faillock module with the following command:

```
# grep -w dir /etc/pam.d/password-auth

auth    required    pam_faillock.so preauth dir=/var/log/faillock
auth    required    pam_faillock.so authfail dir=/var/log/faillock
```

Check the security context type of the non-default tally directory with the following command:

```
# ls -Zd /var/log/faillock

unconfined_u:object_r:faillog_t:s0 /var/log/faillock
```

If the security context type of the non-default tally directory is not "faillog\_t", this is a finding.

**Remediation:**

Configure the OS to allow the use of a non-default faillock tally directory while SELinux enforces a targeted policy.

Update the /etc/selinux/targeted/contexts/files/file\_contexts.local with "faillog\_t" context type for the non-default faillock tally directory with the following command:

```
# semanage fcontext -a -t faillog_t "/var/log/faillock(/.*)?"
```

Next, update the context type of the non-default faillock directory/subdirectories and files with the following command:

```
# restorecon -R -v /var/log/faillock
```

**References:**

1. NIST SP 800-53 :: AC-7 a
2. NIST SP 800-53A :: AC-7.1 (ii)
3. NIST SP 800-53 Revision 5 :: AC-7 b

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-250316  
RULE ID: SV-250316r854080  
STIG ID: RHEL-08-020028  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                      | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>6.2 <u>Establish an Access Revoking Process</u></b><br>Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. |  |  |  |
| v7               | <b>16.7 <u>Establish Process for Revoking Access</u></b><br>Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.                |                                                                                     |  |  |

### 5.3.3.2 Configure pam\_pwquality module

The `pam_pwquality.so` module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more.

These checks are configurable by either:

- use of the module arguments
- modifying the `/etc/security/pwquality.conf` configuration file
- creating a `.conf` file in the `/etc/security/pwquality.conf.d/` directory.

**Note:**

- The module arguments override the settings in the `/etc/security/pwquality.conf` configuration file.
- Settings in the `/etc/security/pwquality.conf` configuration file override settings in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory.

### *5.3.3.2.1 Ensure password number of changed characters is configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The **pwquality difok** option sets the number of characters in a password that must not be present in the old password.

#### **Rationale:**

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

## Audit:

Run the following command to verify that the **difok** option is set to **2** or more and follows local site policy:

```
# grep -Psi -- '^\\h*difok\\h*=\\h*([2-9]|[1-9][0-9]+)\\b'
/etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf
```

*Example output:*

```
/etc/security/pwquality.conf.d/50-pwdifok.conf:difok = 2
```

Verify returned value(s) are **2** or more and meet local site policy

Run the following command to verify that **difok** is not set, is **2** or more, and conforms to local site policy:

```
grep -Psi --
'^\\h*password\\h+(requisite|required|sufficient)\\h+pam_pwquality\\.so\\h+([^\n\r]+\\h+)?difok\\h*=\\h*([0-1])\\b' /etc/pam.d/system-auth /etc/pam.d/password-auth
```

Nothing should be returned

## Notes:

- settings should be configured in only **one** location for clarity
- Settings observe an order of precedence:
  - module arguments override the settings in the **/etc/security/pwquality.conf** configuration file
  - settings in the **/etc/security/pwquality.conf** configuration file override settings in a **.conf** file in the **/etc/security/pwquality.conf.d/** directory
  - settings in a **.conf** file in the **/etc/security/pwquality.conf.d/** directory are read in canonical order, with last read file containing the setting taking precedence
- It is recommended that settings be configured in a **.conf** file in the **/etc/security/pwquality.conf.d/** directory for clarity, convenience, and durability.

## Remediation:

Create or modify a file ending in **.conf** in the **/etc/security/pwquality.conf.d/** directory or the file **/etc/security/pwquality.conf** and add or modify the following line to set **difok** to **2** or more. Ensure setting conforms to local site policy:

```
difok = 2
```

### Example:

```
# sed -ri 's/^\s*difok\s*=/# &/' /etc/security/pwquality.conf
# printf '\n%s' "difok = 2" >> /etc/security/pwquality.conf.d/50-pwdifok.conf
```

Run the following script to remove setting **difok** on the **pam\_pwquality.so** module in the PAM files:

```
#!/usr/bin/env bash

{
    for l_pam_file in system-auth password-auth; do
        l_authselect_file="/etc/authselect/$(head -1
/etc/authselect/authselect.conf | grep 'custom/')/$l_pam_file"
        sed -ri
's/(\s*\s*password\s+(requisite|required|sufficient)\s+pam_pwquality\.so.*) (\s+
difok\s*=\s*\S+) (.*)/\1\4/' "$l_authselect_file"
    done
    authselect apply-changes
}
```

## Default Value:

difok = 1

## References:

1. NIST SP 800-53 Rev. 5: IA-5

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                       |  |  |



**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                                                        | Tactics | Mitigations |
|------------------------------------------------------------------------------------|---------|-------------|
| T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004 | TA0006  | M1027       |

### *5.3.3.2.2 Ensure password length is configured (Automated)*

**Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

**Description:**

**minlen** - Minimum acceptable size for the new password (plus one if credits are not disabled which is the default). Cannot be set to lower value than 6.

**Rationale:**

Strong passwords protect systems from being hacked through brute force methods.

## Audit:

Run the following command to verify that password length is **14** or more characters, and conforms to local site policy:

```
# grep -Psi -- '^h*minlen\h*=\h*(1[4-9]|[2-9][0-9]|[1-9][0-9]{2,})\b' /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf
```

*Example output:*

```
/etc/security/pwquality.conf.d/50-pwlength.conf:minlen = 14
```

Verify returned value(s) are no less than **14** characters and meet local site policy

Run the following command to verify that **minlen** is not set, or is **14** or more characters, and conforms to local site policy:

```
grep -Psi -- '^h*password\h+(requisite|required)sufficient)\h+pam_pwquality\.so\h+([\^#\n\r]+\h+)?minlen\h*=\h*([0-9]|1[0-3])\b' /etc/pam.d/system-auth /etc/pam.d/password-auth
```

Nothing should be returned

## Notes:

- settings should be configured in only **one** location for clarity
- Settings observe an order of precedence:
  - module arguments override the settings in the **/etc/security/pwquality.conf** configuration file
  - settings in the **/etc/security/pwquality.conf** configuration file override settings in a **.conf** file in the **/etc/security/pwquality.conf.d/** directory
  - settings in a **.conf** file in the **/etc/security/pwquality.conf.d/** directory are read in canonical order, with last read file containing the setting taking precedence
- It is recommended that settings be configured in a **.conf** file in the **/etc/security/pwquality.conf.d/** directory for clarity, convenience, and durability.

## Remediation:

Create or modify a file ending in **.conf** in the **/etc/security/pwquality.conf.d/** directory or the file **/etc/security/pwquality.conf** and add or modify the following line to set password length of **14** or more characters. Ensure that password length conforms to local site policy:

*Example:*

```
# sed -ri 's/^\s*minlen\s*=/# &/' /etc/security/pwquality.conf
# printf '\n%s' "minlen = 14" >> /etc/security/pwquality.conf.d/50-
pwlength.conf
```

Run the following script to remove setting **minlen** on the **pam\_pwquality.so** module in the PAM files:

```
#!/usr/bin/env bash

{
    for l_pam_file in system-auth password-auth; do
        l_authselect_file="/etc/authselect/$(head -1
/etc/authselect/authselect.conf | grep 'custom/')/$l_pam_file"
        sed -ri
's/(\s*\s*password\s+(requisite|required|sufficient)\s+pam_pwquality\.so.*) (\s+
minlen\s*=\s*[0-9]+) (.*$)/\1\4/' "$l_authselect_file"
        done
        authselect apply-changes
    }
}
```

## Default Value:

minlen = 8

## References:

1. pam\_pwquality(8)
2. NIST SP 800-53 Rev. 5: IA-5

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                       |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                                                        | Tactics | Mitigations |
|------------------------------------------------------------------------------------|---------|-------------|
| T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004 | TA0006  | M1027       |

### 5.3.3.2.3 *Ensure password complexity is configured (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Password complexity can be set through:

- **minclass** - The minimum number of classes of characters required in a new password. (digits, uppercase, lowercase, others). e.g. **minclass = 4** requires digits, uppercase, lower case, and special characters.
- **dcredit** - The maximum credit for having digits in the new password. If less than 0 it is the minimum number of digits in the new password. e.g. **dcredit = -1** requires at least one digit
- **ucredit** - The maximum credit for having uppercase characters in the new password. If less than 0 it is the minimum number of uppercase characters in the new password. e.g. **ucredit = -1** requires at least one uppercase character
- **ocredit** - The maximum credit for having other characters in the new password. If less than 0 it is the minimum number of other characters in the new password. e.g. **ocredit = -1** requires at least one special character
- **lcredit** - The maximum credit for having lowercase characters in the new password. If less than 0 it is the minimum number of lowercase characters in the new password. e.g. **lcredit = -1** requires at least one lowercase character

#### **Rationale:**

Strong passwords protect systems from being hacked through brute force methods.

## Audit:

Run the following command to verify that complexity conforms to local site policy:

```
# grep -Psi -- '^\\h*(minclass|[dulo]credit)\\b' /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf
```

*Example output:*

```
/etc/security/pwquality.conf.d/50-pwcomplexity.conf:minclass = 4
-- AND/OR --
/etc/security/pwquality.conf.d/50-pwcomplexity.conf:dcredit = -1
/etc/security/pwquality.conf.d/50-pwcomplexity.conf:ucredit = -1
/etc/security/pwquality.conf.d/50-pwcomplexity.conf:ocredit = -1
/etc/security/pwquality.conf.d/50-pwcomplexity.conf:lccredit = -1
```

Run the following command to verify that:

- **minclass** is not set to less than 4
- **dcredit**, **ucredit**, **lccredit**, and **ocredit** are not set to 0 or greater

```
grep -Psi --
'^\\h*password\\h+(requisite|required|sufficient)\\h+pam_pwquality\\.so\\h+([^#\\n\\
r]+\\h+)?(minclass=[0-3]|[dulo]credit=[^-]\\d*)\\b' /etc/pam.d/system-auth
/etc/pam.d/password-auth
```

Nothing should be returned

## Notes:

- settings should be configured in only **one** location for clarity
- Settings observe an order of precedence:
  - module arguments override the settings in the **/etc/security/pwquality.conf** configuration file
  - settings in the **/etc/security/pwquality.conf** configuration file override settings in a **.conf** file in the **/etc/security/pwquality.conf.d/** directory
  - settings in a **.conf** file in the **/etc/security/pwquality.conf.d/** directory are read in canonical order, with last read file containing the setting taking precedence
- It is recommended that settings be configured in a **.conf** file in the **/etc/security/pwquality.conf.d/** directory for clarity, convenience, and durability.

## Remediation:

Create or modify a file ending in **.conf** in the **/etc/security/pwquality.conf.d/** directory or the file **/etc/security/pwquality.conf** and add or modify the following line to set:

- **minclass = 4**

### --AND/OR--

- **dcredit = -\_N\_**
- **ucredit = -\_N\_**
- **ocredit = -\_N\_**
- **lcredit = -\_N\_**

### Example:

```
# sed -ri 's/^\s*minclass\s*=/# &/' /etc/security/pwquality.conf
# printf '\n%s' "minclass = 4" >> /etc/security/pwquality.conf.d/50-
pwcomplexity.conf
```

### --AND/OR--

```
# sed -ri 's/^\s*[dulo]credit\s*=/# &/' /etc/security/pwquality.conf
# printf '%s\n' "dcredit = -1" "ucredit = -1" "ocredit = -1" "lcredit = -1" >
/etc/security/pwquality.conf.d/50-pwcomplexity.conf
```

Run the following script to remove setting **minclass**, **dcredit**, **ucredit**, **lcredit**, and **ocredit** on the **pam\_pwquality.so** module in the PAM files

```
#!/usr/bin/env bash

{
    for l_pam_file in system-auth password-auth; do
        l_authselect_file="/etc/authselect/$(head -1
/etc/authselect/authselect.conf | grep 'custom/')/$l_pam_file"
        sed -ri
's/(^\s*password\s+(requisite|required|sufficient)\s+pam_pwquality\.so.*) (\s+
minclass\s*=\s*\S+) (.*)/\1\4/' "$l_authselect_file"
        sed -ri
's/(^\s*password\s+(requisite|required|sufficient)\s+pam_pwquality\.so.*) (\s+
dcredit\s*=\s*\S+) (.*)/\1\4/' "$l_authselect_file"
        sed -ri
's/(^\s*password\s+(requisite|required|sufficient)\s+pam_pwquality\.so.*) (\s+
ucredit\s*=\s*\S+) (.*)/\1\4/' "$l_authselect_file"
        sed -ri
's/(^\s*password\s+(requisite|required|sufficient)\s+pam_pwquality\.so.*) (\s+
lcredit\s*=\s*\S+) (.*)/\1\4/' "$l_authselect_file"
        sed -ri
's/(^\s*password\s+(requisite|required|sufficient)\s+pam_pwquality\.so.*) (\s+
ocredit\s*=\s*\S+) (.*)/\1\4/' "$l_authselect_file"
    done
    authselect apply-changes
}
```



**Default Value:**

minclass = 0

dcredit = 0

ucredit = 0

ocredit = 0

lcredit = 0

**References:**

1. pam\_pwquality(8)
2. PWQUALITY.CONF(5)
3. NIST SP 800-53 Rev. 5: IA-5

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                       |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                                                        | Tactics | Mitigations |
|------------------------------------------------------------------------------------|---------|-------------|
| T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004 | TA0006  | M1027       |

#### *5.3.3.2.4 Ensure password same consecutive characters is configured (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation
- STIG

##### **Description:**

The `pwquality maxrepeat` option sets the maximum number of allowed same consecutive characters in a new password.

##### **Rationale:**

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

## Audit:

Run the following command to verify that the **maxrepeat** option is set to **3** or less, not **0**, and follows local site policy:

```
# grep -Psi -- '^h*maxrepeat\h*=\h*[1-3]\b' /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf
```

*Example output:*

```
/etc/security/pwquality.conf.d/50-pwrepeat.conf:maxrepeat = 3
```

Verify returned value(s) are **3** or less, not **0**, and meet local site policy

Run the following command to verify that **maxrepeat** is not set, is **3** or less, not **0**, and conforms to local site policy:

```
grep -Psi --
'^h*password\h+(requisite|required|sufficient)\h+pam_pwquality\.so\h+([\#\n\
r]+\h+)?maxrepeat\h*=\h*(0|[4-9]|[1-9][0-9]+)\b' /etc/pam.d/system-auth
/etc/pam.d/password-auth
```

Nothing should be returned

## Notes:

- settings should be configured in only **one** location for clarity
- Settings observe an order of precedence:
  - module arguments override the settings in the **/etc/security/pwquality.conf** configuration file
  - settings in the **/etc/security/pwquality.conf** configuration file override settings in a **.conf** file in the **/etc/security/pwquality.conf.d/** directory
  - settings in a **.conf** file in the **/etc/security/pwquality.conf.d/** directory are read in canonical order, with last read file containing the setting taking precedence
- It is recommended that settings be configured in a **.conf** file in the **/etc/security/pwquality.conf.d/** directory for clarity, convenience, and durability.

## Remediation:

Create or modify a file ending in **.conf** in the **/etc/security/pwquality.conf.d/** directory or the file **/etc/security/pwquality.conf** and add or modify the following line to set **maxrepeat** to **3** or less and not **0**. Ensure setting conforms to local site policy:

*Example:*

```
# sed -ri 's/^\s*maxrepeat\s*=/# &/' /etc/security/pwquality.conf
# printf '\n%s' "maxrepeat = 3" >> /etc/security/pwquality.conf.d/50-
pwrepeat.conf
```

Run the following script to remove setting **maxrepeat** on the **pam\_pwquality.so** module in the PAM files:

```
#!/usr/bin/env bash

{
    for l_pam_file in system-auth password-auth; do
        l_authselect_file="/etc/authselect/$(head -1
/etc/authselect/authselect.conf | grep 'custom/')/$l_pam_file"
        sed -ri
's/ (^\s*password\s+(requisite|required|sufficient)\s+pam_pwquality\.so.*) (\s+
maxrepeat\s*=\s*\S+) (.*)/\1\4/' "$l_authselect_file"
    done
    authselect apply-changes
}
```

## Default Value:

maxrepeat = 0

## References:

1. NIST SP 800-53 :: IA-5 (1) (b)
2. NIST SP 800-53A :: IA-5 (1).1 (v)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230361  
RULE ID: SV-230361r858779  
STIG ID: RHEL-08-020150  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques                                                        | Tactics | Mitigations |
|------------------------------------------------------------------------------------|---------|-------------|
| T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004 | TA0006  | M1027       |

### *5.3.3.2.5 Ensure password maximum sequential characters is configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `pwquality maxsequence` option sets the maximum length of monotonic character sequences in the new password. Examples of such sequence are `12345` or `fedcb`. The check is disabled if the value is `0`.

**Note:** Most such passwords will not pass the simplicity check unless the sequence is only a minor part of the password.

#### **Rationale:**

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

## Audit:

Run the following command to verify that the **maxsequence** option is set to **3** or less, not **0**, and follows local site policy:

```
# grep -Psi -- '^h*maxsequenceh*=\h*[1-3]\b' /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf
```

*Example output:*

```
/etc/security/pwquality.conf.d/50-pwmaxsequence.conf:maxsequence = 3
```

Verify returned value(s) are **3** or less, not **0**, and meet local site policy

Run the following command to verify that **maxsequence** is not set, is **3** or less, not **0**, and conforms to local site policy:

```
grep -Psi --
'^h*passwordh+(requisite|required|sufficient)\h+pam_pwquality\.so\h+([\^#\n\
r]+\h+)?maxsequenceh*=\h*(0|[4-9]|[1-9][0-9]+)\b' /etc/pam.d/system-auth
/etc/pam.d/password-auth
```

Nothing should be returned

## Note:

- settings should be configured in only **one** location for clarity
- Settings observe an order of precedence:
  - module arguments override the settings in the **/etc/security/pwquality.conf** configuration file
  - settings in the **/etc/security/pwquality.conf** configuration file override settings in a **.conf** file in the **/etc/security/pwquality.conf.d/** directory
  - settings in a **.conf** file in the **/etc/security/pwquality.conf.d/** directory are read in canonical order, with last read file containing the setting taking precedence
- It is recommended that settings be configured in a **.conf** file in the **/etc/security/pwquality.conf.d/** directory for clarity, convenience, and durability.

## Remediation:

Create or modify a file ending in **.conf** in the **/etc/security/pwquality.conf.d/** directory or the file **/etc/security/pwquality.conf** and add or modify the following line to set **maxsequence** to **3** or less and not **0**. Ensure setting conforms to local site policy:

*Example:*

```
# sed -ri 's/^\s*maxsequence\s*=/# &/' /etc/security/pwquality.conf
# printf '\n%s' "maxsequence = 3" >> /etc/security/pwquality.conf.d/50-
pwmmaxsequence.conf
```

Run the following script to remove setting **maxsequence** on the **pam\_pwquality.so** module in the PAM files:

```
#!/usr/bin/env bash

{
    for l_pam_file in system-auth password-auth; do
        l_authselect_file="/etc/authselect/$(head -1
/etc/authselect/authselect.conf | grep 'custom/')/$l_pam_file"
        sed -ri
's/(\s*\s*password\s+(requisite|required|sufficient)\s+pam_pwquality\.so.*) (\s+
maxsequence\s*=\s*\S+) (.*)/\1\4/' "$l_authselect_file"
    done
    authselect apply-changes
}
```

## Default Value:

maxsequence = 0

## References:

1. NIST SP 800-53 Rev. 5: IA-5

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                       |  |  |



**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                                                        | Tactics | Mitigations |
|------------------------------------------------------------------------------------|---------|-------------|
| T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004 | TA0006  | M1027       |

### *5.3.3.2.6 Ensure password dictionary check is enabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `pwquality dictcheck` option sets whether to check for the words from the `cracklib` dictionary.

#### **Rationale:**

If the operating system allows the user to select passwords based on dictionary words, this increases the chances of password compromise by increasing the opportunity for successful guesses, and brute-force attacks.

## Audit:

Run the following command to verify that the **dictcheck** option is not set to **0** (disabled) in a pwquality configuration file:

```
# grep -Psi -- '^\\h*dictcheck\\h*==\\h*0\\b' /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf
```

Nothing should be returned

Run the following command to verify that the **dictcheck** option is not set to **0** (disabled) as a module argument in a PAM file:

```
# grep -Psi --
'^\\h*password\\h+(requisite|required|sufficient)\\h+pam_pwquality\\.so\\h+([^\n\
r]+\h+)?dictcheck\\h*==\\h*0\\b' /etc/pam.d/system-auth /etc/pam.d/password-auth
```

Nothing should be returned

## Notes:

- Settings observe an order of precedence:
  - module arguments override the settings in the **/etc/security/pwquality.conf** configuration file
  - settings in the **/etc/security/pwquality.conf** configuration file override settings in a **.conf** file in the **/etc/security/pwquality.conf.d/** directory
  - settings in a **.conf** file in the **/etc/security/pwquality.conf.d/** directory are read in canonical order, with last read file containing the setting taking precedence
- It is recommended that settings be configured in a **.conf** file in the **/etc/security/pwquality.conf.d/** directory for clarity, convenience, and durability.

## Remediation:

Edit any file ending in **.conf** in the **/etc/security/pwquality.conf.d/** directory and/or the file **/etc/security/pwquality.conf** and comment out or remove any instance of **dictcheck = 0**:

*Example:*

```
# sed -ri 's/^\s*dictcheck\s*=/# &/' /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf
```

Run the following script to remove setting **dictcheck** on the **pam\_pwquality.so** module in the PAM files:

```
#!/usr/bin/env bash

{
    for l_pam_file in system-auth password-auth; do
        l_authselect_file="/etc/authselect/$(head -1
/etc/authselect/authselect.conf | grep 'custom/')/$l_pam_file"
        sed -ri
's/(^\s*password\s+(requisite|required|sufficient)\s+pam_pwquality\.so.*) (\s+
dictcheck\s*=\s*\S+) (.*)/\1\4/' "$l_authselect_file"
    done
    authselect apply-changes
}
```

## Default Value:

dictcheck = 1

## References:

1. NIST SP 800-53 Rev. 5: IA-5

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                       |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                                                        | Tactics | Mitigations |
|------------------------------------------------------------------------------------|---------|-------------|
| T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004 | TA0006  | M1027       |

### *5.3.3.2.7 Ensure password quality is enforced for the root user (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

If the `pwquality enforce_for_root` option is enabled, the module will return error on failed check even if the user changing the password is root.

This option is off by default which means that just the message about the failed check is printed but root can change the password anyway.

**Note:** The root is not asked for an old password so the checks that compare the old and new password are not performed.

#### **Rationale:**

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

## Audit:

Run the following command to verify that the `enforce_for_root` option is enabled in a pwquality configuration file:

```
# grep -Psi -- '^h*enforce_for_root\b' /etc/security/pwquality.conf  
/etc/security/pwquality.conf.d/*.conf
```

*Example output:*

```
/etc/security/pwquality.conf.d/50-pwroot.conf:enforce_for_root
```

## Notes:

- Settings observe an order of precedence:
  - module arguments override the settings in the `/etc/security/pwquality.conf` configuration file
  - settings in the `/etc/security/pwquality.conf` configuration file override settings in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory
  - settings in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory are read in canonical order, with last read file containing the setting taking precedence
- It is recommended that settings be configured in a `.conf` file in the `/etc/security/pwquality.conf.d/` directory for clarity, convenience, and durability.

## Remediation:

Edit or add the following line in a `*.conf` file in `/etc/security/pwquality.conf.d` or in `/etc/security/pwquality.conf`:

*Example:*

```
printf '\n%s\n' "enforce_for_root" >> /etc/security/pwquality.conf.d/50-  
pwroot.conf
```

## Default Value:

disabled

## References:

1. NIST SP 800-53 Rev. 5: IA-5

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 <u>Use Unique Passwords</u></b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 <u>Use Unique Passwords</u></b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |



### *5.3.3.2.8 Ensure the operating system enforces a minimum 15-character password length (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Passwords must have a minimum of 15 characters.

#### **Rationale:**

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to increase exponentially the time and/or resources required to compromise the password.

RHEL 8 operating systems utilize "pwquality" as a mechanism to enforce password complexity. Configurations are set in the "etc/security/pwquality.conf" file.

The "minlen", sometimes noted as minimum length, acts as a "score" of complexity based on the credit components of the "pwquality" module. By setting the credit components to a negative value, not only will those components be required, they will not count towards the total "score" of "minlen". This will enable "minlen" to require a 15-character minimum.

The DoD minimum password requirement is 15 characters.

#### **Audit:**

Verify the operating system enforces a minimum 15-character password length. The "minlen" option sets the minimum number of characters in a new password. Check for the value of the "minlen" option in "/etc/security/pwquality.conf" with the following command:

```
# grep -r minlen /etc/security/pwquality.conf*  
  
/etc/security/pwquality.conf:minlen = 15
```

If the command does not return a "minlen" value of 15 or greater, this is a finding.

**Remediation:**

Configure operating system to enforce a minimum 15-character password length.  
Add the following line to "/etc/security/pwquality.conf" (or modify the line to have the required value):

```
minlen = 15
```

**References:**

- 1. NIST SP 800-53 :: IA-5 (1) (a)
- 2. NIST SP 800-53A :: IA-5 (1).1 (i)

**Additional Information:**

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230369

Rule ID: SV-230369r858785

STIG ID: RHEL-08-020230

Severity: CAT II

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1        | IG 2        | IG 3        |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-------------|-------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. | <div></div> | <div></div> | <div></div> |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |             | <div></div> | <div></div> |

### 5.3.3.2.9 Ensure ucredit is configured in /etc/security/pwquality.conf (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must enforce password complexity by requiring that at least one uppercase character be used.

#### Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

RHEL 8 operating systems utilize pwquality as a mechanism to enforce password complexity. Note that in order to require uppercase characters, without degrading the "minlen" value, the credit value must be expressed as a negative number in "/etc/security/pwquality.conf".

#### Audit:

Verify the value for "ucredit" in "/etc/security/pwquality.conf" with the following command:

```
# grep ucredit /etc/security/pwquality.conf
ucredit = -1
```

If the value of "ucredit" is a positive number or is commented out, this is a finding.

#### Remediation:

Configure the operating system to enforce password complexity by requiring that at least one uppercase character be used by setting the "ucredit" option.

Add the following line to /etc/security/pwquality.conf (or modify the line to have the required value):

```
ucredit = -1
```

#### References:

1. NIST SP 800-53 :: IA-5 (1) (a)
2. NIST SP 800-53A :: IA-5 (1).1 (v)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230357  
RULE ID: SV-230357r858771  
STIG ID: RHEL-08-020110  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

### 5.3.3.2.10 Ensure lcredit is configured in /etc/security/pwquality.conf (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must enforce password complexity by requiring that at least one lower-case character be used.

#### Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

RHEL 8 operating systems utilize pwquality as a mechanism to enforce password complexity. Note that in order to require lower-case characters without degrading the "minlen" value, the credit value must be expressed as a negative number in "/etc/security/pwquality.conf".

#### Audit:

Verify the value for "lcredit" in "/etc/security/pwquality.conf" with the following command:

```
# grep lcredit /etc/security/pwquality.conf  
lcredit = -1
```

If the value of "lcredit" is a positive number or is commented out, this is a finding.

#### Remediation:

Configure the operating system to enforce password complexity by requiring that at least one lower-case character be used by setting the "lcredit" option.

Add the following line to /etc/security/pwquality.conf (or modify the line to have the required value):

```
lcredit = -1
```

#### References:

1. NIST SP 800-53 :: IA-5 (1) (a)
2. NIST SP 800-53A :: IA-5 (1).1 (v)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230358  
RULE ID: SV-230358r858773  
STIG ID: RHEL-08-020120  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

### 5.3.3.2.11 Ensure dcredit is configured in /etc/security/pwquality.conf (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must enforce password complexity by requiring that at least one numeric character be used.

#### Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

RHEL 8 operating systems utilize "pwquality" as a mechanism to enforce password complexity. Note that in order to require numeric characters, without degrading the minlen value, the credit value must be expressed as a negative number in "/etc/security/pwquality.conf".

#### Audit:

Verify the value for "dcredit" in "/etc/security/pwquality.conf" with the following command:

```
# grep dcredit /etc/security/pwquality.conf  
dcredit = -1
```

If the value of "dcredit" is a positive number or is commented out, this is a finding.

#### Remediation:

Configure the operating system to enforce password complexity by requiring that at least one numeric character be used by setting the "dcredit" option.

Add the following line to /etc/security/pwquality.conf (or modify the line to have the required value):

```
dcredit = -1
```

#### References:

1. NIST SP 800-53 :: IA-5 (1) (a)
2. NIST SP 800-53A :: IA-5 (1).1 (v)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230359  
RULE ID: SV-230359r858775  
STIG ID: RHEL-08-020130  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |



### 5.3.3.2.12 Ensure ocredit is configured in /etc/security/pwquality.conf (Automated)

#### Profile Applicability:

- STIG

#### Description:

Passwords must contain at least one special character.

#### Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

RHEL 8 operating systems utilize "pwquality" as a mechanism to enforce password complexity. Note that to require special characters without degrading the "minlen" value, the credit value must be expressed as a negative number in "/etc/security/pwquality.conf".

#### Audit:

Verify the value for "ocredit" in "/etc/security/pwquality.conf" with the following command:

```
# grep ocredit /etc/security/pwquality.conf
ocredit = -1
```

If the value of "ocredit" is a positive number or is commented out, this is a finding.

#### Remediation:

Configure the operating system to enforce password complexity by requiring that at least one special character be used by setting the "ocredit" option.

Add the following line to /etc/security/pwquality.conf (or modify the line to have the required value):

```
ocredit = -1
```

#### References:

1. NIST SP 800-53 :: IA-5 (1) (a)
2. NIST SP 800-53A :: IA-5 (1).1 (v)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230375  
RULE ID: SV-230375r858787  
STIG ID: RHEL-08-020280  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

### 5.3.3.2.13 Ensure maxclassrepeat is configured in /etc/security/pwquality.conf (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must require the maximum number of repeating characters of the same character class be limited to four when passwords are changed.

#### Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

RHEL 8 operating systems utilize "pwquality" as a mechanism to enforce password complexity. The "maxclassrepeat" option sets the maximum number of allowed same consecutive characters in the same class in the new password.

#### Audit:

Check for the value of the "maxclassrepeat" option in "/etc/security/pwquality.conf" with the following command:

```
# grep maxclassrepeat /etc/security/pwquality.conf
maxclassrepeat = 4
```

If the value of "maxclassrepeat" is set to more than "4" or is commented out, this is a finding.

#### Remediation:

Configure the operating system to require the change of the number of repeating characters of the same character class when passwords are changed by setting the "maxclassrepeat" option.

Add the following line to "/etc/security/pwquality.conf" conf (or modify the line to have the required value):

```
maxclassrepeat = 4
```

## References:

1. NIST SP 800-53 :: IA-5 (1) (b)
2. NIST SP 800-53A :: IA-5 (1).1 (v)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230360  
RULE ID: SV-230360r858777  
STIG ID: RHEL-08-020140  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |    |    |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

### 5.3.3.2.14 Ensure minclass is configured in /etc/security/pwquality.conf (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must require the change of at least four character classes when passwords are changed.

#### Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

RHEL 8 operating system utilize "pwquality" as a mechanism to enforce password complexity. The "minclass" option sets the minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others).

#### Audit:

Verify the value of the "minclass" option in "/etc/security/pwquality.conf" with the following command:

```
# grep minclass /etc/security/pwquality.conf  
minclass = 4
```

If the value of "minclass" is set to less than "4" or is commented out, this is a finding.

#### Remediation:

Configure the operating system to require the change of at least four character classes when passwords are changed by setting the "minclass" option.

Add the following line to "/etc/security/pwquality.conf" (or modify the line to have the required value):

```
minclass = 4
```

#### References:

1. NIST SP 800-53 :: IA-5 (1) (b)
2. NIST SP 800-53A :: IA-5 (1).1 (v)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230362  
RULE ID: SV-230362r858781  
STIG ID: RHEL-08-020160  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

### 5.3.3.2.15 Ensure difok is configured in /etc/security/pwquality.conf (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must require the change of at least 8 characters when passwords are changed.

#### Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

RHEL 8 operating systems utilize "pwquality" as a mechanism to enforce password complexity. The "difok" option sets the number of characters in a password that must not be present in the old password.

#### Audit:

Verify the value of the "difok" option in "/etc/security/pwquality.conf" with the following command:

```
# grep difok /etc/security/pwquality.conf  
  
difok = 8
```

If the value of "difok" is set to less than "8" or is commented out, this is a finding.

#### Remediation:

Configure the operating system to require the change of at least eight of the total number of characters when passwords are changed by setting the "difok" option. Add the following line to "/etc/security/pwquality.conf" (or modify the line to have the required value):

```
difok = 8
```

#### References:

1. NIST SP 800-53 :: IA-5 (1) (b)
2. NIST SP 800-53A :: IA-5 (1).1 (v)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230363  
RULE ID: SV-230363r858783  
STIG ID: RHEL-08-020170  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |



### 5.3.3.2.16 *Ensure dictcheck is configured (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must prevent the use of dictionary words for passwords.

#### **Rationale:**

If the operating system allows the user to select passwords based on dictionary words, this increases the chances of password compromise by increasing the opportunity for successful guesses, and brute-force attacks.

#### **Audit:**

Verify the operating system prevents the use of dictionary words for passwords. Determine if the field "dictcheck" is set in the "/etc/security/pwquality.conf" or "/etc/pwquality.conf.d/\*.conf" files with the following command:

```
# grep dictcheck /etc/security/pwquality.conf /etc/pwquality.conf.d/*.conf  
  
dictcheck=1
```

If the "dictcheck" parameter is not set to "1", or is commented out, this is a finding.

#### **Remediation:**

Configure the operating system to prevent the use of dictionary words for passwords. Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the /etc/pwquality.conf.d/ directory to contain the "dictcheck" parameter:

```
dictcheck=1
```

#### **References:**

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230377  
RULE ID: SV-230377r858789  
STIG ID: RHEL-08-020300  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

### 5.3.3.2.17 Ensure retry is configured on the pam\_pwquality module in /etc/pam.d/system-auth (Automated)

#### Profile Applicability:

- STIG

#### Description:

RHEL 8 systems below version 8.4 must ensure the password complexity module in the system-auth file is configured for three retries or less.

#### Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. "pwquality" enforces complex password construction configuration and has the ability to limit brute-force attacks on the system.

RHEL 8 uses "pwquality" as a mechanism to enforce password complexity. This is set in both: /etc/pam.d/password-auth /etc/pam.d/system-auth

By limiting the number of attempts to meet the pwquality module complexity requirements before returning with an error, the system will audit abnormal attempts at password changes.

#### Audit:

**Note:** This requirement applies to RHEL versions 8.0 through 8.3. If the system is RHEL version 8.4 or newer, this requirement is not applicable. Verify the operating system is configured to limit the "pwquality" retry option to 3. Check for the use of the "pwquality" retry option in the system-auth file with the following command:

```
# cat /etc/pam.d/system-auth | grep pam_pwquality  
password requisite pam_pwquality.so retry=3
```

If the value of "retry" is set to "0" or greater than "3", this is a finding.

Remediation:

Configure the operating system to limit the "pwquality" retry option to 3.  
Add the following line to the "/etc/pam.d/system-auth" file (or modify the line to have the required value):

```
password requisite pam_pwquality.so retry=3
```

References:

- 1. NIST SP 800-53 :: CM-6 b
- 2. NIST SP 800-53A :: CM-6.1 (iv)

Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024  
  
GROUP ID: V-251714  
RULE ID: SV-251714r902743  
STIG ID: RHEL-08-020102  
SEVERITY: CAT II

CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1        | IG 2        | IG 3        |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-------------|-------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. | <div></div> | <div></div> | <div></div> |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |             | <div></div> | <div></div> |

### 5.3.3.2.18 Ensure retry is configured on the pam\_pwquality module in /etc/pam.d/password-auth (Automated)

#### Profile Applicability:

- STIG

#### Description:

RHEL 8 systems below version 8.4 must ensure the password complexity module in the system-auth file is configured for three retries or less.

#### Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. "pwquality" enforces complex password construction configuration and has the ability to limit brute-force attacks on the system.

RHEL 8 uses "pwquality" as a mechanism to enforce password complexity. This is set in both: /etc/pam.d/password-auth /etc/pam.d/system-auth

By limiting the number of attempts to meet the pwquality module complexity requirements before returning with an error, the system will audit abnormal attempts at password changes.

#### Audit:

**Note:** This requirement applies to RHEL versions 8.0 through 8.3. If the system is RHEL version 8.4 or newer, this requirement is not applicable.

Verify the operating system is configured to limit the "pwquality" retry option to 3. Check for the use of the "pwquality" retry option in the password-auth file with the following command:

```
# cat /etc/pam.d/password-auth | grep pam_pwquality  
password requisite pam_pwquality.so retry=3
```

If the value of "retry" is set to "0" or greater than "3", this is a finding.

**Remediation:**

Configure the operating system to limit the "pwquality" retry option to 3.  
Add the following line to the "/etc/pam.d/password-auth" file (or modify the line to have the required value):

```
password requisite pam_pwquality.so retry=3
```

**References:**

- 1. NIST SP 800-53 :: CM-6 b
- 2. NIST SP 800-53A :: CM-6.1 (iv)

**Additional Information:**

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024  
  
GROUP ID: V-251715  
RULE ID: SV-251715r902746  
STIG ID: RHEL-08-020103  
SEVERITY: CAT II

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1        | IG 2        | IG 3        |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-------------|-------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. | <div></div> | <div></div> | <div></div> |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |             | <div></div> | <div></div> |

### 5.3.3.2.19 Ensure retry is configured in /etc/security/pwquality.conf (Automated)

#### Profile Applicability:

- STIG

#### Description:

RHEL 8 systems, version 8.4 and above, must ensure the password complexity module is configured for three retries or less.

#### Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. "pwquality" enforces complex password construction configuration and has the ability to limit brute-force attacks on the system.

RHEL 8 utilizes "pwquality" as a mechanism to enforce password complexity. This is set in both: /etc/pam.d/password-auth /etc/pam.d/system-auth By limiting the number of attempts to meet the pwquality module complexity requirements before returning with an error, the system will audit abnormal attempts at password changes.

#### Audit:

**Note:** This requirement applies to RHEL versions 8.4 or newer. If the system is RHEL below version 8.4, this requirement is not applicable.

Verify the operating system is configured to limit the "pwquality" retry option to 3.

Check for the use of the "pwquality" retry option with the following command:

```
# grep -r retry /etc/security/pwquality.conf*  
  
/etc/security/pwquality.conf:retry = 3
```

If the value of "retry" is set to "0" or greater than "3", is commented out or missing, this is a finding.

If conflicting results are returned, this is a finding.

Check for the use of the "pwquality" retry option in the system-auth and password-auth files with the following command:

```
# grep pwquality /etc/pam.d/system-auth /etc/pam.d/password-auth | grep retry
```

If the command returns any results, this is a finding.

**Remediation:**

Configure the operating system to limit the "pwquality" retry option to 3.  
Add the following line to the "/etc/security/pwquality.conf" file(or modify the line to have the required value):

```
retry = 3
```

Remove any configurations that conflict with the above value.

**References:**

- 1. NIST SP 800-53 :: CM-6 b
- 2. NIST SP 800-53A :: CM-6.1 (iv)

**Additional Information:**

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-251716  
RULE ID: SV-251716r858737  
STIG ID: RHEL-08-020104  
SEVERITY: CAT II

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                       |  |  |



### 5.3.3.3 Configure pam\_pwhistory module

**pam\_pwhistory** - PAM module to remember last passwords

**pam\_history.so** module - This module saves the last passwords for each user in order to force password change history and keep the user from alternating between the same password too frequently.

This module does not work together with kerberos. In general, it does not make much sense to use this module in conjunction with **NIS** or **LDAP**, since the old passwords are stored on the local machine and are not available on another machine for password history checking.

Options:

- **debug** - Turns on debugging via syslog(3).
- **use\_authtok** - When password changing enforce the module to use the new password provided by a previously stacked password module (this is used in the example of the stacking of the **pam\_passwdqc** module documented below).
- **enforce\_for\_root** - If this option is set, the check is enforced for root, too.
- **remember=<N>** - The last <N> passwords for each user are saved. The default is **10**. Value of **0** makes the module to keep the existing contents of the `opasswd` file unchanged.
- **retry=<N>** - Prompt user at most <N> times before returning with error. The default is **1**.
- **authtok\_type=<STRING>** - See `pam_get_authtok(3)` for more details.
- **conf=</path/to/config-file>** - Use another configuration file instead of the default `/etc/security/pwhistory.conf`.

*Examples:*

An example password section would be:

```
##PAM-1.0
password      required      pam_pwhistory.so
password      required      pam_unix.so          use_authtok
```

In combination with `pam_passwdqc`:

```
##PAM-1.0
password      required      pam_passwdqc.so    config=/etc/passwdqc.conf
password      required      pam_pwhistory.so    use_authtok
password      required      pam_unix.so          use_authtok
```

The options for configuring the module behavior are described in the `pwhistory.conf(5)` manual page. The options specified on the module command line override the values from the configuration file.

`pwhistory.conf` provides a way to configure the default settings for saving the last passwords for each user. This file is read by the `pam_pwhistory` module and is the preferred method over configuring `pam_pwhistory` directly.

The file has a very simple `name = value` format with possible comments starting with `#` character. The whitespace at the beginning of line, end of line, and around the `=` sign is ignored.

Options:

- `debug` - Turns on debugging via `syslog(3)`.
- `enforce_for_root` - If this option is set, the check is enforced for root, too.
- `remember=<N>` - The last `<N>` passwords for each user are saved. The default is `10`. Value of `0` makes the module to keep the existing contents of the `opasswd` file unchanged.
- `retry=<N>` - Prompt user at most `<N>` times before returning with error. The default is `1`.
- `file=</path/filename>` - Store password history in file `</path/filename>` rather than the default location. The default location is `/etc/security/opasswd`.

### 5.3.3.3.1 Ensure password history remember is configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The `/etc/security/opasswd` file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords. The number of passwords remembered is set via the `remember` argument value in `set` for the `pam_pwhistory` module.

- `remember=<N>` - `<N>` is the number of old passwords to remember

#### Rationale:

Requiring users not to reuse their passwords make it less likely that an attacker will be able to guess the password or use a compromised password.

**Note:** These change only apply to accounts configured on the local system.

#### Audit:

Run the following command and verify that the `remember` option is set to **24** or more and meets local site policy in `/etc/security/pwhistory.conf`:

```
# grep -Pi -- '^h*rememberh*=\h*(2[4-9]|[3-9][0-9]|[1-9][0-9]{2,})\b'
/etc/security/pwhistory.conf

remember = 24
```

Run the following command to verify that the `remember` option is not set to less than **24** on the `pam_pwhistory.so` module in `/etc/pam.d/password-auth` and `/etc/pam.d/system-auth`:

```
# grep -Pi --
'^h*passwordh+(requisite|required|sufficient)\h+pam_pwhistory\.so\h+([\^#\n\r]+\h+)?remember=(2[0-3]|1[0-9]|[0-9])\b' /etc/pam.d/system-auth
/etc/pam.d/password-auth

Nothing should be returned
```

Remediation:

Edit or add the following line in `/etc/security/pwhistory.conf`:

```
remember = 24
```

Run the following script to remove the `remember` argument from the `pam_pwhistory.so` module in `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth`:

```
#!/usr/bin/env bash

{
  for l_pam_file in system-auth password-auth; do
    l_authselect_file="/etc/authselect/$(head -1
/etc/authselect/authselect.conf | grep 'custom/')/$l_pam_file"
    sed -ri
's/(\s*password\s+(requisite|required|sufficient)\s+pam_pwhistory\.so.*) (\s+
remember\s*=\s*\S+) (.*$) /\1\4/' "$l_authselect_file"
  done
  authselect apply-changes
}
```

References:

- 1. NIST SP 800-53 Rev. 5: IA-5(1)

CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                       |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                                                  | Tactics | Mitigations |
|------------------------------------------------------------------------------|---------|-------------|
| T1078, T1078.001,<br>T1078.002, T1078.003,<br>T1078.004, T1110,<br>T1110.004 |         |             |

### 5.3.3.3.2 Ensure password history is enforced for the root user (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

If the `pwhistory enforce_for_root` option is enabled, the module will enforce password history for the root user as well

#### Rationale:

Requiring users not to reuse their passwords make it less likely that an attacker will be able to guess the password or use a compromised password

**Note:** These change only apply to accounts configured on the local system.

#### Audit:

Run the following command to verify that the `enforce_for_root` option is enabled in `/etc/pwhistory.conf`:

```
# grep -Pi -- '^h*enforce_for_root\b' /etc/security/pwhistory.conf
enforce_for_root
```

#### Notes:

- Settings observe an order of precedence.
- Module arguments override the settings in the `/etc/security/pwhistory.conf` configuration file
- It is recommended that settings be configured in `/etc/security/pwhistory.conf` for clarity, convenience, and durability.

#### Remediation:

Edit or add the following line in `/etc/security/pwhistory.conf`:

```
enforce_for_root
```

#### Default Value:

disabled

#### References:

1. NIST SP 800-53 Rev. 5: IA-5

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques                                                        | Tactics | Mitigations |
|------------------------------------------------------------------------------------|---------|-------------|
| T1110, T1110.001, T1110.002, T1110.003, T1178.001, T1178.002, T1178.003, T1178.004 | TA0006  | M1027       |

### 5.3.3.3.3 Ensure pam\_pwhistory includes use\_authtok (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

**use\_authtok** - When password changing enforce the module to set the new password to the one provided by a previously stacked password module

#### Rationale:

**use\_authtok** allows multiple pam modules to confirm a new password before it is accepted.

#### Audit:

Run the following command to verify that **use\_authtok** is set on the **pam\_pwhistory.so** module lines in the password stack:

```
# grep -P --  
'^\h*password\h+([\^#\n\r]+\)\h+pam_pwhistory\.so\h+([\^#\n\r]+\h+)?use_authtok\  
b' /etc/pam.d/{password,system}-auth
```

Output should be similar to:

```
/etc/pam.d/password-auth:password    required    pam_pwhistory.so use_authtok  
/etc/pam.d/system-auth:password    required    pam_pwhistory.so use_authtok
```

Verify that the lines include **use\_authtok**

#### Remediation:

Run the following script to verify the active authselect profile includes **use\_authtok** on the password stack's **pam\_pwhistory.so** module lines:



```
#!/usr/bin/env bash

{
    l_pam_profile="$(head -1 /etc/authselect/authselect.conf)"
    if grep -Pq -- '^custom\/' <<< "$l_pam_profile"; then
        l_pam_profile_path="/etc/authselect/$l_pam_profile"
    else
        l_pam_profile_path="/usr/share/authselect/default/$l_pam_profile"
    fi
    grep -P --
'^\h*password\h+(requisite|required|sufficient)\h+pam_pwhistory\.so\h+([\#\n\r]+\h+)?use_authtok\b' "$l_pam_profile_path"/{password,system}-auth
}
```

*Example output:*

```
/etc/authselect/custom/custom-profile/password-auth:password    required
pam_pwhistory.so use_authtok

/etc/authselect/custom/custom-profile/system-auth:password    required
pam_pwhistory.so use_authtok
```

**- IF -** the output does not include **use\_authtok**, run the following script:

```
#!/usr/bin/env bash

{
    l_pam_profile="$(head -1 /etc/authselect/authselect.conf)"
    if grep -Pq -- '^custom\/' <<< "$l_pam_profile"; then
        l_pam_profile_path="/etc/authselect/$l_pam_profile"
    else
        l_pam_profile_path="/usr/share/authselect/default/$l_pam_profile"
    fi
    for l_authselect_file in "$l_pam_profile_path"/password-auth
"$l_pam_profile_path"/system-auth; do
        if grep -Pq
'^\h*password\h+([\#\n\r]+\h+pam_pwhistory\.so\h+([\#\n\r]+\h+)?use_authtok\b' "$l_authselect_file"; then
            echo "- \"use_authtok\" is already set"
        else
            echo "- \"use_authtok\" is not set. Updating template"
            sed -ri
's/(^\s*password\s+(requisite|required|sufficient)\s+pam_pwhistory\.so\s+.*)$
/& use_authtok/g' "$l_authselect_file"
        fi
    done
}
```

Run the following command to update the **password-auth** and **system-auth** files in **/etc/pam.d** to include the **use\_authtok** argument on the password stack's **pam\_pwhistory.so** lines:

```
# authselect apply-changes
```

## References:

1. NIST SP 800-53 Rev. 5: IA-5

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.11 <u>Encrypt Sensitive Data at Rest</u></b><br>Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data. |      |  |  |
| v7               | <b>16.4 <u>Encrypt or Hash all Authentication Credentials</u></b><br>Encrypt or hash with a salt all authentication credentials when stored.                                                                                                                                                                                                                                                                                                                                    |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1003, T1003.008, T1110, T1110.002 | TA0006  | M1041       |

#### 5.3.3.3.4 Ensure remember is configured on the pam\_pwhistory module in /etc/pam.d/password-auth (Automated)

##### **Profile Applicability:**

- STIG

##### **Description:**

Passwords must be prohibited from reuse for a minimum of five generations.

##### **Rationale:**

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. If the information system or application allows the user to reuse their password consecutively when that password has exceeded its defined lifetime, the end result is a password that is not changed per policy requirements.

RHEL 8 operating system's utilize "pwquality" consecutively as a mechanism to enforce password complexity. This is set in both: /etc/pam.d/password-auth /etc/pam.d/system-auth.

Note that manual changes to the listed files may be overwritten by the "authselect" program.

##### **Audit:**

Verify the operating system prohibits password reuse for a minimum of five generations. Check for the value of the "remember" argument in "/etc/pam.d/password-auth" with the following command:

```
# grep -i remember /etc/pam.d/password-auth  
password requisite pam_pwhistory.so use_authtok remember=5 retry=3
```

If the line containing "pam\_pwhistory.so" does not have the "remember" module argument set, is commented out, or the value of the "remember" module argument is set to less than "5", this is a finding.

## Remediation:

Configure the operating system in the password-auth file to prohibit password reuse for a minimum of five generations.

Add the following line in "/etc/pam.d/password-auth" (or modify the line to have the required value):

```
password requisite pam_pwhistory.so use_authtok remember=5 retry=3
```

## References:

1. NIST SP 800-53 :: IA-5 (1) (e)
2. NIST SP 800-53A :: IA-5 (1).1 (v)

## Additional Information:

```
Red Hat Enterprise Linux 8
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230368
RULE ID: SV-230368r902759
STIG ID: RHEL-08-020220
SEVERITY: CAT II
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>16 Account Monitoring and Control</b><br>Account Monitoring and Control                                                                                                                                                                     |                                                                                       |                                                                                       |                                                                                       |

### 5.3.3.3.5 Ensure remember is configured on the pam\_pwhistory module in /etc/pam.d/system-auth (Automated)

#### Profile Applicability:

- STIG

#### Description:

The Operating System (OS) must be configured in the system-auth file to prohibit password reuse for a minimum of five generations.

#### Rationale:

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. If the information system or application allows the user to reuse their password consecutively when that password has exceeded its defined lifetime, the end result is a password that is not changed per policy requirements.

RHEL 8 uses "pwhistory" consecutively as a mechanism to prohibit password reuse. This is set in both: /etc/pam.d/password-auth /etc/pam.d/system-auth.

Note that manual changes to the listed files may be overwritten by the "authselect" program.

#### Audit:

Verify the operating system is configured in the system-auth file to prohibit password reuse for a minimum of five generations.

Check for the value of the "remember" argument in "/etc/pam.d/system-auth" with the following command:

```
# grep -i remember /etc/pam.d/system-auth  
password requisite pam_pwhistory.so use_authtok remember=5 retry=3
```

If the line containing "pam\_pwhistory.so" does not have the "remember" module argument set, is commented out, or the value of the "remember" module argument is set to less than "5", this is a finding.

## Remediation:

Configure the operating system in the system-auth file to prohibit password reuse for a minimum of five generations.

Add the following line in "/etc/pam.d/system-auth" (or modify the line to have the required value):

```
password requisite pam_pwhistory.so use_authtok remember=5 retry=3
```

## References:

1. NIST SP 800-53 :: IA-5 (1) (e)
2. NIST SP 800-53A :: IA-5 (1).1 (v)

## Additional Information:

```
Red Hat Enterprise Linux 8
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-251717
RULE ID: SV-251717r902749
STIG ID: RHEL-08-020221
SEVERITY: CAT II
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                       |  |  |

#### 5.3.3.4 Configure pam\_unix module

The `pam_unix.so` module is the standard Unix authentication module. It uses standard calls from the system's libraries to retrieve and set account information as well as authentication. Usually this is obtained from the `/etc/passwd` and the `/etc/shadow` file as well if shadow is enabled.

### 5.3.3.4.1 Ensure pam\_unix does not include nullok (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The **nullok** argument overrides the default action of **pam\_unix.so** to not permit the user access to a service if their official password is blank.

#### Rationale:

Using a strong password is essential to helping protect personal and sensitive information from unauthorized access

#### Audit:

Run the following command to verify that the **nullok** argument is not set on the **pam\_unix.so** module:

```
# grep -P --  
'^\h*(auth|account|password|session)\h+(requisite|required|sufficient)\h+pam_  
unix\.so\b' /etc/pam.d/{password,system}-auth
```

Verify that none of the returned lines includes **nullok**. Output should be similar to:

```
/etc/pam.d/password-auth:auth    sufficient    pam_unix.so  
/etc/pam.d/password-auth:account required      pam_unix.so  
/etc/pam.d/password-auth:password sufficient     pam_unix.so sha512 shadow  
use_authtok  
/etc/pam.d/password-auth:session required        pam_unix.so  
  
/etc/pam.d/system-auth:auth    sufficient    pam_unix.so  
/etc/pam.d/system-auth:account required        pam_unix.so  
/etc/pam.d/system-auth:password sufficient       pam_unix.so sha512 shadow  
use_authtok  
/etc/pam.d/system-auth:session required           pam_unix.so
```



## Remediation:

Run the following script to verify that the active authselect profile's **system-auth** and **password-auth** files include **{if not "without-nullok":nullok}** - **OR** - don't include the **nullok** option on the **pam\_unix.so** module:

```
{
  l_module_name="unix"
  l_profile_name="$(head -1 /etc/authselect/authselect.conf)"
  if [[ ! "$l_profile_name" =~ ^custom\/* ]]; then
    echo " - Follow Recommendation \"Ensure custom authselect profile is used\" and then return to this Recommendation"
  else
    grep -P -- "\bpam_${l_module_name}\.so\b"
    /etc/authselect/${l_profile_name}/{password,system}-auth
  fi
}
```

*Example output with a custom profile named "custom-profile":*

```
/etc/authselect/custom/custom-profile/password-auth:auth    sufficient
pam_unix.so {if not "without-nullok":nullok}
/etc/authselect/custom/custom-profile/password-auth:account  required
pam_unix.so
/etc/authselect/custom/custom-profile/password-auth:password  sufficient
pam_unix.so sha512 shadow {if not "without-nullok":nullok} use_authok
/etc/authselect/custom/custom-profile/password-auth:session  required
pam_unix.so

/etc/authselect/custom/custom-profile/system-auth:auth    sufficient
pam_unix.so {if not "without-nullok":nullok}
/etc/authselect/custom/custom-profile/system-auth:account  required
pam_unix.so
/etc/authselect/custom/custom-profile/system-auth:password  sufficient
pam_unix.so sha512 shadow {if not "without-nullok":nullok} use_authok
/etc/authselect/custom/custom-profile/system-auth:session  required
pam_unix.so
```

- **IF** - any line is returned with **nullok** that doesn't also include **{if not "without-nullok":nullok}**, run the following script:

```
#!/usr/bin/env bash

{
  for l_pam_file in system-auth password-auth; do
    l_file="/etc/authselect/$(head -1 /etc/authselect/authselect.conf |
grep 'custom/')/${l_pam_file}"
    sed -ri
's/(^\s*password\s+(requisite|required|sufficient)\s+pam_unix\.so\s+.*)(nullok)
(\s*.*)$/\1\2\4/g' $l_file
  done
}
```

- **IF** - any line is returned with **{if not "without-nullok":nullok}**, run the following command to enable the authselect **without-nullok** feature:

```
# authselect enable-feature without-nullok
```

Run the following command to update the files in `/etc/pam.d` to include `pam_unix.so` without the `nullok` argument:

```
# authselect apply-changes
```

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

```
Red Hat Enterprise Linux 8
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-244540
RULE ID: SV-244540r743869
STIG ID: RHEL-08-020331
SEVERITY: CAT I

GROUP ID: V-244541
RULE ID: SV-244541r743872
STIG ID: RHEL-08-020332
SEVERITY: CAT I
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                       |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1003, T1003.008, T1110, T1110.002 | TA0006  | M1041       |

### 5.3.3.4.2 Ensure pam\_unix does not include remember (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The `remember=n` argument saves the last `n` passwords for each user in `/etc/security/opasswd` in order to force password change history and keep the user from alternating between the same password too frequently. The MD5 password hash algorithm is used for storing the old passwords. Instead of this option the `pam_pwhistory` module should be used. The `pam_pwhistory` module saves the last `n` passwords for each user in `/etc/security/opasswd` using the password hash algorithm set on the `pam_unix` module. This allows for the `sha512` hash algorithm to be used.

#### Rationale:

The `remember=n` argument should be removed to ensure a strong password hashing algorithm is being used. A stronger hash provides additional protection to the system by increasing the level of effort needed for an attacker to successfully determine local user's old passwords stored in `/etc/security/opasswd`.

#### Audit:

Run the following command to verify that the `remember` argument is not set on the `pam_unix.so` module:

```
# grep -Pi '^h*password\h+([\^#\n\r]+\h+)?pam_unix\.so\b'
/etc/pam.d/{password,system}-auth | grep -Pv '\bremember=\d\b'
```

Output should be similar to:

```
/etc/pam.d/password-auth:password    sufficient    pam_unix.so sha512 shadow
use_authok

/etc/pam.d/system-auth:password      sufficient    pam_unix.so sha512 shadow
use_authok
```

## Remediation:

Run the following script to verify the active authselect profile doesn't include the **remember** argument on the **pam\_unix.so** module lines:

```
#!/usr/bin/env bash

{
  l_pam_profile="$(head -1 /etc/authselect/authselect.conf)"
  if grep -Pq -- '^custom\/' <<< "$l_pam_profile"; then
    l_pam_profile_path="/etc/authselect/$l_pam_profile"
  else
    l_pam_profile_path="/usr/share/authselect/default/$l_pam_profile"
  fi
  grep -P -- '^h*password\h+([\#\n\r]+\h+)pam_unix\.so\b'
"$l_pam_profile_path"/{password,system}-auth
}
```

Output should be similar to:

```
/etc/authselect/custom/custom-profile/password-auth:password    sufficient
pam_unix.so sha512 shadow {if not "without-nullok":nullok} use_authtok

/etc/authselect/custom/custom-profile/system-auth:password    sufficient
pam_unix.so sha512 shadow {if not "without-nullok":nullok} use_authtok
```

- **IF** - any line includes **remember=**, run the following script to remove the **remember=** from the **pam\_unix.so** lines in the active authselect profile **password-auth** and **system-auth** templates:

```
#!/usr/bin/env bash

{
  l_pam_profile="$(head -1 /etc/authselect/authselect.conf)"
  if grep -Pq -- '^custom\/' <<< "$l_pam_profile"; then
    l_pam_profile_path="/etc/authselect/$l_pam_profile"
  else
    l_pam_profile_path="/usr/share/authselect/default/$l_pam_profile"
  fi
  for l_authselect_file in "$l_pam_profile_path"/password-auth
"$l_pam_profile_path"/system-auth; do
    sed -ri
's/(^s*password\s+(requisite|required|sufficient)\s+pam_unix\.so\s+.*)(remember=[1-9][0-9]*) (\s*.*)$/\1\4/g' "$l_authselect_file"
  done
}
```

Run the following command to update the **password-auth** and **system-auth** files in **/etc/pam.d** to include **pam\_unix.so** without the **remember** argument:

```
# authselect apply-changes
```

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1003, T1003.008, T1110, T1110.002 | TA0006  | M1041       |

### 5.3.3.4.3 Ensure pam\_unix includes a strong password hashing algorithm (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

A cryptographic hash function converts an arbitrary-length input into a fixed length output. Password hashing performs a one-way transformation of a password, turning the password into another string, called the hashed password.

#### Rationale:

The **SHA-512** and **yescrypt** algorithms provide a stronger hash than other algorithms used by Linux for password hash generation. A stronger hash provides additional protection to the system by increasing the level of effort needed for an attacker to successfully determine local user passwords.

**Note:** These changes only apply to the local system.

#### Audit:

**Note:** **yescrypt** is not currently supported in Fedora 28 based distributions. It has been included as an acceptable option if it becomes available in a future update to the Operating System.

Run the following command to verify that a strong password hashing algorithm is set on the pam\_unix.so module:

```
# grep -P --  
'^\h*password\h+([\#\n\r]+\h+pam_unix\.so\h+([\#\n\r]+\h+)?(sha512|yescrypt)  
\b' /etc/pam.d/{password,system}-auth
```

Output should be similar to:

```
/etc/pam.d/password-auth:password    sufficient    pam_unix.so sha512 shadow  
use_authok  
  
/etc/pam.d/system-auth:password    sufficient    pam_unix.so sha512 shadow  
use_authok
```

Verify that the lines include either **sha512** - **OR** - **yescrypt**

## Remediation:

### Notes:

- If **yescrypt** becomes available in a future release, this would also be acceptable. It is highly recommended that the chosen hashing algorithm is consistent across **/etc/libuser.conf**, **/etc/login.defs**, **/etc/pam.d/password-auth**, and **/etc/pam.d/system-auth**.
- This only effects local users and passwords created after updating the files to use **sha512** or **yescrypt**. If it is determined that the password algorithm being used is not **sha512** or **yescrypt**, once it is changed, it is recommended that all user ID's be immediately expired and forced to change their passwords on next login.

Run the following script to verify the active authselect profile includes a strong password hashing algorithm on the password stack's **pam\_unix.so** module lines:

```
#!/usr/bin/env bash

{
  l_pam_profile="$(head -1 /etc/authselect/authselect.conf) "
  if grep -Pq -- '^custom\/' <<< "$l_pam_profile"; then
    l_pam_profile_path="/etc/authselect/$l_pam_profile"
  else
    l_pam_profile_path="/usr/share/authselect/default/$l_pam_profile"
  fi
  grep -P --
  '^\\h*password\\h+(requisite|required)sufficient)\\h+pam_unix\\.so\\h+([^\n\r]+\h
+)?(sha512|yescrypt)\\b' "$l_pam_profile_path"/{password,system}-auth
}
```

### Example output:

```
/etc/authselect/custom/custom-profile/password-auth:password sufficient
pam_unix.so sha512 shadow {if not "without-nullok":nullok} use_authtok

/etc/authselect/custom/custom-profile/system-auth:password sufficient
pam_unix.so sha512 shadow {if not "without-nullok":nullok} use_authtok
```

**- IF -** the output does not include either **sha512** - **OR - yescrypt**, or includes a different hashing algorithm, run the following script:

```
#!/usr/bin/env bash

{
    l_pam_profile="$(head -1 /etc/authselect/authselect.conf)"
    if grep -Pq -- '^custom\/' <<< "$l_pam_profile"; then
        l_pam_profile_path="/etc/authselect/$l_pam_profile"
    else
        l_pam_profile_path="/usr/share/authselect/default/$l_pam_profile"
    fi
    for l_authselect_file in "$l_pam_profile_path"/password-auth
"$l_pam_profile_path"/system-auth; do
        if grep -Pq
'^\h*password\h+(\h+pam_unix\.so\h+([\h#\n\r]+\h+)?(sha512|yescrypt)\b'
"$l_authselect_file"; then
            echo "- A strong password hashing algorithm is correctly set"
        elif grep -Pq
'^\h*password\h+(\h+pam_unix\.so\h+([\h#\n\r]+\h+)?(md5|bigcrypt|sha256|blowf
ish)\b' "$l_authselect_file"; then
            echo "- A weak password hashing algorithm is set, updating to
\"sha512\""
            sed -ri
's/(\h*s*password\s+(requisite|required|sufficient)\s+pam_unix\.so\s+.*)(md5|b
igcrypt|sha256|blowfish)(\s*.*)$/\1\4 sha512/g' "$l_authselect_file"
        else
            echo "No password hashing algorithm is set, updating to \"sha512\""
            sed -ri
's/(\h*s*password\s+(requisite|required|sufficient)\s+pam_unix\.so\s+.*)$/&
sha512/g' "$l_authselect_file"
        fi
    done
}
```

Run the following command to update the **password-auth** and **system-auth** files in **/etc/pam.d** to include **pam\_unix.so** with a strong password hashing algorithm argument:

```
# authselect apply-changes
```

## References:

1. NIST SP 800-53 Rev. 5: IA-5



## Additional Information:

Additional module options may be set, recommendation only covers those listed here.

The following command may be used to expire all non-system user ID's immediately and force them to change their passwords on next login. Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems.

```
# awk -F: ' ( $3<"$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)" && $1 != "nfsnobody" ) { print $1 }' /etc/passwd | xargs -n 1 chage -d 0
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.11 <u>Encrypt Sensitive Data at Rest</u></b><br>Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data. |      |    |    |
| v7               | <b>16.4 <u>Encrypt or Hash all Authentication Credentials</u></b><br>Encrypt or hash with a salt all authentication credentials when stored.                                                                                                                                                                                                                                                                                                                                    |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1003, T1003.008, T1110, T1110.002 | TA0006  | M1041       |

#### 5.3.3.4.4 Ensure pam\_unix includes use\_authtok (Automated)

##### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

##### Description:

**use\_authtok** - When password changing enforce the module to set the new password to the one provided by a previously stacked password module

##### Rationale:

**use\_authtok** allows multiple pam modules to confirm a new password before it is accepted.

##### Audit:

Run the following command to verify that **use\_authtok** is set on the **pam\_unix.so** module lines in the password stack:

```
# grep -P --  
'^\h*password\h+([\h*\n\r]+\h+pam_unix\.so\h+([\h*\n\r]+\h+)?use_authtok\b'  
/etc/pam.d/{password,system}-auth
```

Output should be similar to:

```
/etc/pam.d/password-auth:password    sufficient    pam_unix.so  sha512 shadow  
use_authtok  
  
/etc/pam.d/system-auth:password    sufficient    pam_unix.so  sha512 shadow  
use_authtok
```

Verify that the lines include **use\_authtok**

##### Remediation:

Run the following script to verify the active authselect profile includes **use\_authtok** on the password stack's **pam\_unix.so** module lines:

```
#!/usr/bin/env bash

{
    l_pam_profile="$(head -1 /etc/authselect/authselect.conf)"
    if grep -Pq -- '^custom\/' <<< "$l_pam_profile"; then
        l_pam_profile_path="/etc/authselect/$l_pam_profile"
    else
        l_pam_profile_path="/usr/share/authselect/default/$l_pam_profile"
    fi
    grep -P --
'^\h*password\h+(requisite|required|sufficient)\h+pam_unix\.so\h+([\#\n\r]+\h
+)?use_authtok\b' "$l_pam_profile_path"/{password,system}-auth
}
```

**Example output:**

```
/etc/authselect/custom/custom-profile/password-auth:password    sufficient
pam_unix.so sha512 shadow {if not "without-nullok":nullok} use_authtok

/etc/authselect/custom/custom-profile/system-auth:password    sufficient
pam_unix.so sha512 shadow {if not "without-nullok":nullok} use_authtok
```

**- IF -** the output does not include **use\_authtok**, run the following script:

```
#!/usr/bin/env bash

{
    l_pam_profile="$(head -1 /etc/authselect/authselect.conf)"
    if grep -Pq -- '^custom\/' <<< "$l_pam_profile"; then
        l_pam_profile_path="/etc/authselect/$l_pam_profile"
    else
        l_pam_profile_path="/usr/share/authselect/default/$l_pam_profile"
    fi
    for l_authselect_file in "$l_pam_profile_path"/password-auth
"$l_pam_profile_path"/system-auth; do
        if grep -Pq
'^\h*password\h+([\#\n\r]+\h+pam_unix\.so\h+([\#\n\r]+\h+)?use_authtok\b'
"$l_authselect_file"; then
            echo "- \"use_authtok\" is already set"
        else
            echo "- \"use_authtok\" is not set. Updating template"
            sed -ri
's/(\h*s*password\h+(requisite|required|sufficient)\h+pam_unix\.so\h+s+.*)$/&
use_authtok/g' "$l_authselect_file"
        fi
    done
}
```

Run the following command to update the **password-auth** and **system-auth** files in **/etc/pam.d** to include the **use\_authtok** argument on the password stack's **pam\_unix.so** lines:

```
# authselect apply-changes
```

## References:

1. NIST SP 800-53 Rev. 5: IA-5

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.11 <u>Encrypt Sensitive Data at Rest</u></b><br>Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data. |      |  |  |
| v7               | <b>16.4 <u>Encrypt or Hash all Authentication Credentials</u></b><br>Encrypt or hash with a salt all authentication credentials when stored.                                                                                                                                                                                                                                                                                                                                    |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1003, T1003.008, T1110, T1110.002 | TA0006  | M1041       |

### 5.3.3.4.5 Ensure pam\_unix includes a FIPS 140-2 approved hashing algorithm (Automated)

#### Profile Applicability:

- STIG

#### Description:

A cryptographic hash function converts an arbitrary-length input into a fixed length output. Password hashing performs a one-way transformation of a password, turning the password into another string, called the hashed password.

#### Rationale:

The **SHA-512** algorithm provides a stronger FIPS 140-2 approved cryptographic hashing algorithm than other algorithms used by Linux for password hash generation. A stronger hash provides additional protection to the system by increasing the level of effort needed for an attacker to successfully determine local user passwords.

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and DoD data may be compromised.

Systems utilizing encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general-purpose computing system.

**Note:** These changes only apply to the local system.

#### Audit:

Run the following command to verify that **sha512** is set on the pam\_unix.so module:

```
# grep -P --  
'^\h*password\h+([\#\n\r]+)\h+pam_unix\.so\h+([\#\n\r]+\h+)?sha512\b'  
/etc/pam.d/{password,system}-auth
```

#### Example Output:

```
/etc/pam.d/password-auth:password    sufficient    pam_unix.so sha512 shadow  
use_authok  
  
/etc/pam.d/system-auth:password    sufficient    pam_unix.so sha512 shadow  
use_authok
```

Verify that the lines include **sha512**

## Remediation:

**Note:** This only effects local users and passwords created after updating the files to use **sha512**. If it is determined that the password algorithm being used is not **sha512**, once it is changed, it is recommended that all user ID's be immediately expired and forced to change their passwords on next login.

Run the following script to verify the active authselect profile includes the **sha512** password hashing algorithm on the password stack's pam\_unix.so module lines:

```
#!/usr/bin/env bash

{
  l_pam_profile="$(head -1 /etc/authselect/authselect.conf)"
  if grep -Pq -- '^custom\/' <<< "$l_pam_profile"; then
    l_pam_profile_path="/etc/authselect/$l_pam_profile"
  else
    l_pam_profile_path="/usr/share/authselect/default/$l_pam_profile"
  fi
  grep -P --
  '^\\h*password\\h+(requisite|required)sufficient\\h+pam_unix\\.so\\h+([^\n\r]+\\h
+)?sha512\\b' "$l_pam_profile_path"/{password,system}-auth
}
```

### *Example output:*

```
/etc/authselect/custom/custom-profile/password-auth:password    sufficient
pam_unix.so sha512 shadow {if not "without-nullok":nullok} use_authtok

/etc/authselect/custom/custom-profile/system-auth:password    sufficient
pam_unix.so sha512 shadow {if not "without-nullok":nullok} use_authtok
```

- **IF** - the output does not include **sha512**, or includes a different hashing algorithm, run the following script:

```
#!/usr/bin/env bash

{
    l_pam_profile="$(head -1 /etc/authselect/authselect.conf)"
    if grep -Pq -- '^custom\/' <<< "$l_pam_profile"; then
        l_pam_profile_path="/etc/authselect/$l_pam_profile"
    else
        l_pam_profile_path="/usr/share/authselect/default/$l_pam_profile"
    fi
    for l_authselect_file in "$l_pam_profile_path"/password-auth
"$l_pam_profile_path"/system-auth; do
        if grep -Pq
'^\h*password\h+()\h+pam_unix\.so\h+([\#\n\r]+\h+)?sha512\b'
"$l_authselect_file"; then
            echo "- The sha512 password hashing algorithm is correctly set"
        elif grep -Pq
'^\h*password\h+()\h+pam_unix\.so\h+([\#\n\r]+\h+)?(md5|bigcrypt|sha256|blowf
ish|yescrypt)\b' "$l_authselect_file"; then
            echo "- An incorrect password hashing algorithm is set, updating to
\"sha512\""
            sed -ri
's/(^\s*password\s+(requisite|required|sufficient)\s+pam_unix\.so\s+.*)(md5|b
igcrypt|sha256|blowfish|yescrypt)(\s*.*)$/\1\4 sha512/g' "$l_authselect_file"
        else
            echo "No password hashing algorithm is set, updating to \"sha512\""
            sed -ri
's/(^\s*password\s+(requisite|required|sufficient)\s+pam_unix\.so\s+.*)$/&
sha512/g' "$l_authselect_file"
        fi
    done
}
```

Run the following command to update the **password-auth** and **system-auth** files in **/etc/pam.d** to include **pam\_unix.so** with the **sha512** password hashing algorithm argument:

```
# authselect apply-changes
```

## References:

1. NIST SP 800-53 :: IA-7
2. NIST SP 800-53A :: IA-7.1

## Additional Information:

Additional module options may be set, recommendation only covers those listed here.

The following command may be used to expire all non-system user ID's immediately and force them to change their passwords on next login. Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems.

```
# awk -F: ' ( $3<"$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)" && $1 != "nfsnobody" ) { print $1 }' /etc/passwd | xargs -n 1 chage -d 0
```

## Red Hat Enterprise Linux 8

```
Red Hat Enterprise Linux 8 STIG
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230237
RULE ID: SV-230237r809276
STIG ID: RHEL-08-010160
SEVERITY: CAT II

GROUP ID: V-244524
RULE ID: SV-244524r809331
STIG ID: RHEL-08-010159
SEVERITY: CAT II
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.11 <u>Encrypt Sensitive Data at Rest</u></b><br>Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data. |      |  |  |
| v7               | <b>16.4 <u>Encrypt or Hash all Authentication Credentials</u></b><br>Encrypt or hash with a salt all authentication credentials when stored.                                                                                                                                                                                                                                                                                                                                    |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1003, T1003.008, T1110, T1110.002 | TA0006  | M1041       |



### 5.3.3.5 Configure pam\_lastlog module

pam\_lastlog is a PAM module to display a line of information about the last login of the user. In addition, the module maintains the `/var/log/lastlog` file.

Some applications may perform this function themselves. In such cases, this module is not necessary.

If the module is called in the auth or account phase, the accounts that were not used recently enough will be disallowed to log in. The check is not performed for the root account, so the root is never locked out.

### *5.3.3.5.1 Ensure the date and time of the last successful account logon upon logon is displayed (Automated)*

**Profile Applicability:**

- STIG

**Description:**

The operating system must display the date and time of the last successful account logon upon logon.

**Rationale:**

Providing users with feedback on when account accesses last occurred facilitates user recognition and reporting of unauthorized account use.

**Audit:**

Verify users are provided with feedback on when account accesses last occurred with the following command:

```
# grep pam_lastlog /etc/pam.d/postlogin  
session required pam_lastlog.so showfailed
```

If "pam\_lastlog" is missing from "/etc/pam.d/postlogin" file, or the silent option is present, this is a finding.

**Remediation:**

Configure the operating system to provide users with feedback on when account accesses last occurred by setting the required configuration options in "/etc/pam.d/postlogin".

Add the following line to the top of "/etc/pam.d/postlogin":

```
session required pam_lastlog.so showfailed
```

**References:**

1. NIST SP 800-53 Revision 5 :: AC-9
2. NIST SP 800-53A :: AC-9.1

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230381  
Rule ID: SV-230381r858726  
STIG ID: RHEL-08-020340  
Severity: CAT III

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### 5.3.3.6 Configure pam\_sss module

pam\_sss.so is the PAM interface to the System Security Services daemon (SSSD). Errors and results are logged through syslog(3) with the LOG\_AUTHPRIV facility.

### *5.3.3.6.1 Ensure the operating system uses multifactor authentication for local access to accounts (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must implement smart card login for multifactor authentication for access to interactive accounts.

#### **Rationale:**

Using an authentication device, such as a Common Access Card (CAC) or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD CAC.

There are various methods of implementing multifactor authentication for RHEL 8. Some methods include a local system multifactor account mapping or joining the system to a domain and utilizing a Red Hat idM server or Microsoft Windows Active Directory server. Any of these methods will require that the client operating system handle the multifactor authentication correctly.

Satisfies: SRG-OS-000105-GPOS-00052, SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000108-GPOS-00055

## Audit:

Verify the operating system uses multifactor authentication for local access to accounts.

**Note:** If the System Administrator demonstrates the use of an approved alternate multifactor authentication method, this requirement is not applicable.

Check that the "pam\_cert\_auth" setting is set to "true" in the "/etc/sss/sssd.conf" file.

Check that the "try\_cert\_auth" or "require\_cert\_auth" options are configured in both "/etc/pam.d/system-auth" and "/etc/pam.d/smartcard-auth" files with the following command:

```
# grep -ir cert_auth /etc/sss/sssd.conf /etc/pam.d/*  
  
/etc/sss/sssd.conf:pam_cert_auth = True  
/etc/pam.d/smartcard-auth:auth sufficient pam_sss.so try_cert_auth  
/etc/pam.d/system-auth:auth [success=done authinfo_unavail=ignore  
ignore=ignore default=die] pam_sss.so try_cert_auth
```

If "pam\_cert\_auth" is not set to "true" in "/etc/sss/sssd.conf", this is a finding.

If "pam\_sss.so" is not set to "try\_cert\_auth" or "require\_cert\_auth" in both the "/etc/pam.d/smartcard-auth" and "/etc/pam.d/system-auth" files, this is a finding.

## Remediation:

Configure the operating system to use multifactor authentication for local access to accounts.

Add or update the "pam\_cert\_auth" setting in the "/etc/sss/sssd.conf" file to match the following line:

```
[pam]  
pam_cert_auth = True
```

Add or update "pam\_sss.so" with "try\_cert\_auth" or "require\_cert\_auth" in the "/etc/pam.d/system-auth" and "/etc/pam.d/smartcard-auth" files based on the following examples:

```
/etc/pam.d/smartcard-auth:auth sufficient pam_sss.so try_cert_auth  
  
/etc/pam.d/system-auth:auth [success=done authinfo_unavail=ignore  
ignore=ignore default=die] pam_sss.so try_cert_auth
```

The "sss" service must be restarted for the changes to take effect. To restart the "sss" service, run the following command:

```
# systemctl restart sss.service
```

## References:

1. NIST SP 800-53 :: IA-2 (1)
2. NIST SP 800-53A :: IA-2 (1).1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230372  
Rule ID: SV-230372r942945  
STIG ID: RHEL-08-020250  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                              | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>6.5 <u>Require MFA for Administrative Access</u></b><br>Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider. |  |  |  |
| v7               | <b>16.3 <u>Require Multi-factor Authentication</u></b><br>Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.                            |                                                                                     |  |  |

### 5.3.3.6.2 Ensure SSSD prohibits the use of cached authentications after one day (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must prohibit the use of cached authentications after one day.

#### Rationale:

If cached authentication information is out-of-date, the validity of the authentication information may be questionable.

The operating system includes multiple options for configuring authentication, but this requirement will be focus on the System Security Services Daemon (SSSD). By default sssd does not cache credentials.

#### Audit:

Verify that the SSSD prohibits the use of cached authentications after one day.

Note: If smart card authentication is not being used on the system this item is Not Applicable.

Check that SSSD allows cached authentications with the following command:

```
# grep -ir cache_credentials /etc/sss/sss.conf /etc/sss/conf.d/*.conf  
  
cache_credentials = true
```

If "cache\_credentials" is set to "false" or missing from the configuration file, this is not a finding and no further checks are required.

If "cache\_credentials" is set to "true", check that SSSD prohibits the use of cached authentications after one day with the following command:

```
# grep -ir offline_credentials_expiration /etc/sss/sss.conf  
/etc/sss/conf.d/*.conf  
  
offline_credentials_expiration = 1
```

If "offline\_credentials\_expiration" is not set to a value of "1", this is a finding.



## Remediation:

Configure the SSSD to prohibit the use of cached authentications after one day.  
Add or change the following line in "/etc/sss/sss.conf" just below the line "[pam]".

```
offline_credentials_expiration = 1
```

## References:

1. NIST SP 800-53 Revision 5 :: IA-5 (13)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230376  
Rule ID: SV-230376r942948  
STIG ID: RHEL-08-020290  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### 5.3.3.6.3 *Ensure the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file (Manual)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must map the authenticated identity to the user or group account for PKI-based authentication.

#### **Rationale:**

Without mapping the certificate used to authenticate to the user account, the ability to determine the identity of the individual user or group will not be available for forensic analysis.

There are various methods of mapping certificates to user/group accounts. For the purposes of this requirement, the check and fix will account for Active Directory mapping. Some of the other possible methods include joining the system to a domain and utilizing a Red Hat idM server, or a local system mapping, where the system is not part of a domain.

#### **Audit:**

Verify the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file with the following command:

```
# cat /etc/sss/sss.conf

[sss]
config_file_version = 2
services = pam, sudo, ssh
domains = testing.test

[pam]
pam_cert_auth = True

[domain/testing.test]
id_provider = ldap

[certmap/testing.test/rule_name]
matchrule =<SAN>.*EDIPI@mil
maprule = (userCertificate;binary={cert!bin})
domains = testing.test
```

If the certmap section does not exist, ask the System Administrator to indicate how certificates are mapped to accounts. If there is no evidence of certificate mapping, this is a finding.

## Remediation:

Configure the operating system to map the authenticated identity to the user or group account by adding or modifying the certmap section of the "/etc/sss/sssd.conf" file based on the following example:

```
[certmap/testing.test/rule_name]
matchrule =<SAN>.*EDIPI@mil
maprule = (userCertificate;binary={cert!bin})
domains = testing.test
```

The "sss" service must be restarted for the changes to take effect. To restart the "sss" service, run the following command:

```
# systemctl restart sss.service
```

## References:

1. NIST SP 800-53 :: IA-5 (2)
2. NIST SP 800-53A :: IA-5 (2).1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230355  
Rule ID: SV-230355r858743  
STIG ID: RHEL-08-020090  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                       | IG 1 | IG 2 | IG 3 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | 6.4 <u>Require MFA for Remote Network Access</u><br>Require MFA for remote network access.                                                                                                                    | ●    | ●    | ●    |
| v8               | 6.5 <u>Require MFA for Administrative Access</u><br>Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider. | ●    | ●    | ●    |
| v7               | 16.3 <u>Require Multi-factor Authentication</u><br>Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.                            |      | ●    | ●    |

## 5.4 User Accounts and Environment

This section provides guidance on setting up secure defaults for system and user accounts and their environment.

### 5.4.1 Configure shadow password suite parameters

While a majority of the password control parameters have been moved to PAM, some parameters are still available through the shadow password suite. Any changes made to `/etc/login.defs` will only be applied if the `usermod` command is used. If user IDs are added a different way, use the `chage` command to effect changes to individual user IDs.

### 5.4.1.1 Ensure password expiration is configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The `PASS_MAX_DAYS` parameter in `/etc/login.defs` allows an administrator to force passwords to expire once they reach a defined age.

`PASS_MAX_DAYS <N>` - The maximum number of days a password may be used. If the password is older than this, a password change will be forced. If not specified, -1 will be assumed (which disables the restriction).

#### Rationale:

The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity.

We recommend a yearly password change. This is primarily because for all their good intentions users will share credentials across accounts. Therefore, even if a breach is publicly identified, the user may not see this notification, or forget they have an account on that site. This could leave a shared credential vulnerable indefinitely. Having an organizational policy of a 1-year (annual) password expiration is a reasonable compromise to mitigate this with minimal user burden.

## Impact:

The password expiration must be greater than the minimum days between password changes or users will be unable to change their password.

Excessive password expiration requirements do more harm than good, because these requirements make users select predictable passwords, composed of sequential words and numbers that are closely related to each other. In these cases, the next password can be predicted based on the previous one (incrementing a number used in the password for example). Also, password expiration requirements offer no containment benefits because attackers will often use credentials as soon as they compromise them. Instead, immediate password changes should be based on key events including, but not limited to:

- Indication of compromise
- Change of user roles
- When a user leaves the organization.

Not only does changing passwords every few weeks or months frustrate the user, but it's also been suggested that it does more harm than good, because it could lead to bad practices by the user such as adding a character to the end of their existing password.

## Audit:

Run the following command and verify **PASS\_MAX\_DAYS** is set to 365 days or less and conforms to local site policy:

```
# grep -Pi -- '^h*PASS_MAX_DAYS\h+\d+\b' /etc/login.defs
```

*Example output:*

```
PASS_MAX_DAYS 365
```

Run the following command to verify all **/etc/shadow** passwords **PASS\_MAX\_DAYS**:

- is greater than **0** days
- is less than or equal to **365** days
- conforms to local site policy

```
# awk -F: '($2~/^\$.+\$/ ) {if($5 > 365 || $5 < 1)print "User: " $1 " " "PASS_MAX_DAYS: " $5}' /etc/shadow
```

Nothing should be returned

## Remediation:

Set the **PASS\_MAX\_DAYS** parameter to conform to site policy in **/etc/login.defs** :

```
PASS_MAX_DAYS 365
```

Modify user parameters for all users with a password set to match:

```
# chage --maxdays 365 <user>
```

Edit **/etc/login.defs** and set **PASS\_MAX\_DAYS** to a value greater than **0** that follows local site policy:

*Example:*

```
PASS_MAX_DAYS 365
```

Run the following command to modify user parameters for all users with a password set to a maximum age no greater than **365** or less than **1** that follows local site policy:

```
# chage --maxdays <N> <user>
```

*Example:*

```
# awk -F: '($2~/^\$.+\/) {if($5 > 365 || $5 < 1)system ("chage --maxdays 365 " $1)}' /etc/shadow
```

**Warning:** If a password has been set at system install or kickstart, the **last change date** field is not set, In this case, setting **PASS\_MAX\_DAYS** will immediately expire the password. One possible solution is to populate the **last change date** field through a command like: **chage -d "\$(date +%Y-%m-%d)" root**

## Default Value:

PASS\_MAX\_DAYS 99999

## References:

1. CIS Password Policy Guide
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## Additional Information:

A value of -1 will disable password expiration.



## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques                                                                          | Tactics | Mitigations |
|------------------------------------------------------------------------------------------------------|---------|-------------|
| T1078, T1078.001, T1078.002, T1078.003, T1078.004, T1110, T1110.001, T1110.002, T1110.003, T1110.004 |         |             |

### *5.4.1.2 Ensure minimum password days is configured (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### **Description:**

**PASS\_MIN\_DAYS** <N> - The minimum number of days allowed between password changes. Any password changes attempted sooner than this will be rejected. If not specified, 0 will be assumed (which disables the restriction).

#### **Rationale:**

Users may have favorite passwords that they like to use because they are easy to remember and they believe that their password choice is secure from compromise. Unfortunately, passwords are compromised and if an attacker is targeting a specific individual user account, with foreknowledge of data about that user, reuse of old, potentially compromised passwords, may cause a security breach.

By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls

#### **Impact:**

If a users password is set by other personnel as a procedure in dealing with a lost or expired password, the user should be forced to update this "set" password with their own password. e.g. force "change at next logon".

If it is not possible to have a user set their own password immediately, and this recommendation or local site procedure may cause a user to continue using a third party generated password, **PASS\_MIN\_DAYS** for the effected user should be temporally changed to 0, to allow a user to change their password immediately.

For applications where the user is not using the password at console, the ability to "change at next logon" may be limited. This may cause a user to continue to use a password created by other personnel.

## Audit:

Run the following command to verify that **PASS\_MIN\_DAYS** is set to a value greater than 0 and follows local site policy:

```
# grep -Pi -- '^\\h*PASS_MIN_DAYS\\h+\\d+\\b' /etc/login.defs
```

*Example output:*

```
PASS_MIN_DAYS 1
```

Run the following command to verify all passwords have a **PASS\_MIN\_DAYS** greater than 0:

```
# awk -F: '($2~/^\\$.+\\$/) {if($4 < 1)print "User: " $1 " PASS_MIN_DAYS: " $4}' /etc/shadow
```

Nothing should be returned

## Remediation:

Edit **/etc/login.defs** and set **PASS\_MIN\_DAYS** to a value greater than 0 that follows local site policy:

*Example:*

```
PASS_MIN_DAYS 1
```

Run the following command to modify user parameters for all users with a password set to a minimum days greater than zero that follows local site policy:

```
# chage --mindays <N> <user>
```

*Example:*

```
# awk -F: '($2~/^\\$.+\\$/) {if($4 < 1)system ("chage --mindays 1 " $1)}' /etc/shadow
```

## Default Value:

PASS\_MIN\_DAYS 0

## References:

1. CIS Password Policy Guide
2. NIST SP 800-53 :: IA-5 (1) (d)
3. NIST SP 800-53A :: IA-5 (1).1 (v)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230364  
RULE ID: SV-230364r627750  
STIG ID: RHEL-08-020180  
SEVERITY: CAT II

Vul ID: V-230365  
Rule ID: SV-230365r858727  
STIG ID: RHEL-08-020190  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |    |    |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques                                         | Tactics | Mitigations |
|---------------------------------------------------------------------|---------|-------------|
| T1078, T1078.001, T1078.002, T1078.003, T1078.004, T1110, T1110.004 | TA0006  | M1027       |

### 5.4.1.3 Ensure password expiration warning days is configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The **PASS\_WARN\_AGE** parameter in **/etc/login.defs** allows an administrator to notify users that their password will expire in a defined number of days.

**PASS\_WARN\_AGE** <N> - The number of days warning given before a password expires. A zero means warning is given only upon the day of expiration, a negative value means no warning is given. If not specified, no warning will be provided.

#### Rationale:

Providing an advance warning that a password will be expiring gives users time to think of a secure password. Users caught unaware may choose a simple password or write it down where it may be discovered.

#### Audit:

Run the following command and verify **PASS\_WARN\_AGE** is 7 or more and follows local site policy:

```
# grep -Pi -- '^h*PASS_WARN_AGE\h+\d+\b' /etc/login.defs
```

*Example output:*

```
PASS_WARN_AGE 7
```

Run the following command to verify all passwords have a **PASS\_WARN\_AGE** of 7 or more:

```
# awk -F: '($2~/^\$.+\$/ ) {if($6 < 7)print "User: " $1 " PASS_WARN_AGE: " $6}' /etc/shadow
```

Nothing should be returned

## Remediation:

Edit `/etc/login.defs` and set `PASS_WARN_AGE` to a value of **7** or more that follows local site policy:

*Example:*

```
PASS_WARN_AGE 7
```

Run the following command to modify user parameters for all users with a password set to a minimum warning to **7** or more days that follows local site policy:

```
# chage --warndays <N> <user>
```

*Example:*

```
# awk -F: '($2~/^\$.+\/) {if($6 < 7)system ("chage --warndays 7 " $1)}' /etc/shadow
```

## Default Value:

`PASS_WARN_AGE 7`

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.1 Establish and Maintain a Secure Configuration Process</b><br>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                                                                                                                                                                                           |                                                                                       |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1078                       | TA0006  | M1027       |

#### 5.4.1.4 Ensure strong password hashing algorithm is configured (Automated)

##### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

##### Description:

A cryptographic hash function converts an arbitrary-length input into a fixed length output. Password hashing performs a one-way transformation of a password, turning the password into another string, called the hashed password.

**ENCRYPT\_METHOD** (string) - This defines the system default encryption algorithm for encrypting passwords (if no algorithm are specified on the command line). It can take one of these values:

- **MD5** - MD5-based algorithm will be used for encrypting password
- **SHA256** - SHA256-based algorithm will be used for encrypting password
- **SHA512** - SHA512-based algorithm will be used for encrypting password
- **BCRYPT** - BCRYPT-based algorithm will be used for encrypting password
- **YESCRYPT** - YESCRYPT-based algorithm will be used for encrypting password
- **DES** - DES-based algorithm will be used for encrypting password (default)

##### Note:

- This parameter overrides the deprecated **MD5\_CRYPT\_ENAB** variable.
- This parameter will only affect the generation of group passwords.
- The generation of user passwords is done by PAM and subject to the PAM configuration.
- It is recommended to set this variable consistently with the PAM configuration.

##### Rationale:

The **SHA-512** and **yescrypt** algorithms provide a stronger hash than other algorithms used by Linux for password hash generation. A stronger hash provides additional protection to the system by increasing the level of effort needed for an attacker to successfully determine local group passwords.

## Audit:

Run the following command to verify the hashing algorithm is **sha512** or **yescrypt** in **/etc/login.defs**:

```
# grep -Pi -- '^\\h*ENCRYPT_METHOD\\h+(SHA512|yescrypt)\\b' /etc/login.defs
```

*Example output:*

```
ENCRYPT_METHOD SHA512
- OR -
ENCRYPT_METHOD YESCRYPT
```

## Remediation:

Edit **/etc/login.defs** and set the **ENCRYPT\_METHOD** to **SHA512** or **YESCRYPT**:

```
ENCRYPT_METHOD <HASHING_ALGORITHM>
```

*Example:*

```
ENCRYPT_METHOD YESCRYPT
```

## Note:

- This only effects local groups' passwords created after updating the file to use **sha512** or **yescrypt**.
- If it is determined that the password algorithm being used is not **sha512** or **yescrypt**, once it is changed, it is recommended that all group passwords be updated to use the stronger hashing algorithm.
- It is recommended that the chosen hashing algorithm is consistent across **/etc/login.defs** and the PAM configuration

## Default Value:

```
ENCRYPT_METHOD SHA512
```

## References:

1. NIST SP 800-53 Rev. 5: IA-5



## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.11 <u>Encrypt Sensitive Data at Rest</u></b><br>Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data. |      |  |  |
| v7               | <b>16.4 <u>Encrypt or Hash all Authentication Credentials</u></b><br>Encrypt or hash with a salt all authentication credentials when stored.                                                                                                                                                                                                                                                                                                                                    |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1003, T1003.008, T1110, T1110.002 | TA0006  | M1041       |

### 5.4.1.5 Ensure inactive password lock is configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

User accounts that have been inactive for over a given period of time can be automatically disabled.

**INACTIVE** - Defines the number of days after the password exceeded its maximum age where the user is expected to replace this password.

The value is stored in the shadow password file. An input of **0** will disable an expired password with no delay. An input of **-1** will blank the respective field in the shadow password file.

#### Rationale:

Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

#### Audit:

Run the following command and verify **INACTIVE** conforms to site policy (no more than 45 days):

```
# useradd -D | grep INACTIVE  
  
INACTIVE=45
```

Verify all users with a password have Password inactive no more than 45 days after password expires

Verify all users with a password have Password inactive no more than 45 days after password expires: Run the following command and Review list of users and **INACTIVE** to verify that all users **INACTIVE** conforms to site policy (no more than 45 days):

```
# awk -F: '($2~/^\$.+\/) {if($7 > 45 || $7 < 0)print "User: " $1 " INACTIVE:  
" $7 "Days"}' /etc/shadow
```

Nothing should be returned

## Remediation:

Run the following command to set the default password inactivity period to 45 days or less that meets local site policy:

```
# useradd -D -f <N>
```

*Example:*

```
# useradd -D -f 45
```

Run the following command to modify user parameters for all users with a password set to a inactive age of 45 days or less that follows local site policy:

```
# chage --inactive <N> <user>
```

*Example:*

```
# awk -F: '($2~/^\$.+\/) {if($7 > 45 || $7 < 0)system ("chage --inactive 45 " $1)}' /etc/shadow
```

## Default Value:

INACTIVE=-1

## References:

1. CIS Password Policy Guide

## Additional Information:

A value of -1 would disable this setting.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                       |  |  |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1078, T1078.002,<br>T1078.003     | TA0001         | M1027              |

### 5.4.1.6 Ensure all users last password change date is in the past (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

All users should have a password change date in the past.

#### Rationale:

If a user's recorded password change date is in the future, then they could bypass any set password expiration.

#### Audit:

Run the following script and verify nothing is returned:

```
#!/usr/bin/env bash

{
  while IFS= read -r l_user; do
    l_change=$(date -d "$(chage --list $l_user | grep '^Last password change' | cut -d: -f2 | grep -v 'never$')" +%s)
    if [[ "$l_change" -gt "$(date +%s)" ]]; then
      echo "User: \"$l_user\" last password change was \"$(chage --list $l_user | grep '^Last password change' | cut -d: -f2)\""
    fi
  done < <(awk -F: '$2~/^\\$.+\\$/{print $1}' /etc/shadow)
}
```

#### Remediation:

Investigate any users with a password change date in the future and correct them. Locking the account, expiring the password, or resetting the password manually may be appropriate.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques                                                                          | Tactics | Mitigations |
|------------------------------------------------------------------------------------------------------|---------|-------------|
| T1078, T1078.001, T1078.002, T1078.003, T1078.004, T1110, T1110.001, T1110.002, T1110.003, T1110.004 |         |             |

### *5.4.1.7 Ensure passwords use FIPS 140-2 approved cryptographic hashing algorithm (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

A cryptographic hash function converts an arbitrary-length input into a fixed length output. Password hashing performs a one-way transformation of a password, turning the password into another string, called the hashed password.

**ENCRYPT\_METHOD** (string) - This defines the system default encryption algorithm for encrypting passwords (if no algorithm are specified on the command line). It can take one of these values:

- **MD5** - MD5-based algorithm will be used for encrypting password
- **SHA256** - SHA256-based algorithm will be used for encrypting password
- **SHA512** - SHA512-based algorithm will be used for encrypting password
- **BCRYPT** - BCRYPT-based algorithm will be used for encrypting password
- **YESCRYPT** - YESCRYPT-based algorithm will be used for encrypting password
- **DES** - DES-based algorithm will be used for encrypting password (default)

#### **Note:**

- This parameter overrides the deprecated **MD5\_CRYPT\_ENAB** variable.
- This parameter will only affect the generation of group passwords.
- The generation of user passwords is done by PAM and subject to the PAM configuration.
- It is recommended to set this variable consistently with the PAM configuration.

## Rationale:

The **SHA-512** algorithm provides a strong FIPS 140-2 approved hash for password hash generation. A stronger hash provides additional protection to the system by increasing the level of effort needed for an attacker to successfully determine local group passwords.

The operating system must encrypt all stored passwords with a FIPS 140-2 approved cryptographic hashing algorithm.

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and data may be compromised.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DoD requirements.

## Audit:

Run the following command to verify the hashing algorithm is **sha512** in **/etc/login.defs**:

```
# grep -Pi -- '^h*ENCRYPT_METHODh+SHA512\b' /etc/login.defs
```

Verify output is:

```
ENCRYPT_METHOD SHA512
```

## Remediation:

Edit **/etc/login.defs** and set the **ENCRYPT\_METHOD** to **SHA512**:

```
ENCRYPT_METHOD SHA512
```

## Note:

- This only effects local groups' passwords created after updating the file to use **sha512**.
- If it is determined that the password algorithm being used is not **sha512**, once it is changed, it is recommended that all group passwords be updated to use the stronger hashing algorithm.
- It is recommended that the chosen hashing algorithm is consistent across **/etc/login.defs** and the PAM configuration

## Default Value:

ENCRYPT\_METHOD SHA512



## References:

1. NIST SP 800-53 Rev. 5: IA-5
2. NIST SP 800-53 :: IA-5 (1) (c)
3. NIST SP 800-53A :: IA-5 (1).1 (v)

## Additional Information:

### Red Hat Enterprise Linux 8

Red Hat Enterprise Linux 8 STIG  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230231  
RULE ID: SV-230231r877397  
STIG ID: RHEL-08-010110  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | IG 1 | IG 2 | IG 3 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.11 <u>Encrypt Sensitive Data at Rest</u></b><br>Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data. |      | ●    | ●    |
| v7               | <b>16.4 <u>Encrypt or Hash all Authentication Credentials</u></b><br>Encrypt or hash with a salt all authentication credentials when stored.                                                                                                                                                                                                                                                                                                                                    |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1003, T1003.008, T1110, T1110.002 | TA0006  | M1041       |

### 5.4.1.8 Ensure minimum number of hashing rounds is configured (Automated)

#### Profile Applicability:

- STIG

#### Description:

When `ENCRYPT_METHOD` is set to `SHA256` or `SHA512`, the `SHA_CRYPT_MIN_ROUNDS` and `SHA_CRYPT_MAX_ROUNDS` parameters define the number of `SHA` rounds used by the encryption algorithm by default when the number of rounds is not specified on the command line.

With a lot of rounds, it is more difficult to brute force the password. But note also that more CPU resources will be needed to authenticate users.

If not specified, the `libc` will choose the default number of rounds (5000), which is orders of magnitude too low for modern hardware.

The values must be inside the 1000-999,999,999 range.

If only one of the `SHA_CRYPT_MIN_ROUNDS` or `SHA_CRYPT_MAX_ROUNDS` values is set, then this value will be used.

If `SHA_CRYPT_MIN_ROUNDS > SHA_CRYPT_MAX_ROUNDS`, the highest value will be used.

**Note:** This parameter only affect the generation of group passwords. The generation of user passwords is done by PAM and subject to the PAM configuration. It is recommended to set this variable consistently with the PAM configuration.

#### Rationale:

The system must use a strong hashing algorithm to store the password. The system must use a sufficient number of hashing rounds to ensure the required level of entropy.

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

#### Impact:

A large number of rounds requires more CPU resources to authenticate users

## Audit:

Run the following command to verify **SHA\_CRYPT\_MIN\_ROUNDS** is set to **5000** or greater:

```
# grep -Psi -- '^\\h*SHA_CRYPT_(MAX|MIN)_ROUNDS\\h+\\d+\\b' /etc/login.defs
```

*Example output:*

```
SHA_CRYPT_MAX_ROUNDS 5000
-AND/OR-
SHA_CRYPT_MIN_ROUNDS 5000
```

**Note:** any value between **5,000** and **1000-999,999,999** is acceptable

## Remediation:

Edit **/etc/login.defs** and add or modify the line containing **SHA\_CRYPT\_MIN\_ROUNDS**:

*Example:*

```
SHA_CRYPT_MIN_ROUNDS 5000
```

## References:

1. NIST SP 800-53 :: IA-5 (1) (c)
2. NIST SP 800-53A :: IA-5 (1).1 (v)
3. LOGIN.DEFS(5)

## Additional Information:

Red Hat Enterprise Linux 8

```
Red Hat Enterprise Linux 8 STIG
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230233
RULE ID: SV-230233r880705
STIG ID: RHEL-08-010130
SEVERITY: CAT II
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.11 <u>Encrypt Sensitive Data at Rest</u></b><br>Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data. |      |  |  |
| v7               | <b>16.4 <u>Encrypt or Hash all Authentication Credentials</u></b><br>Encrypt or hash with a salt all authentication credentials when stored.                                                                                                                                                                                                                                                                                                                                    |      |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1003, T1003.008, T1110, T1110.002 | TA0006  | M1041       |

#### *5.4.1.9 Ensure existing passwords use FIPS 140-2 approved cryptographic hashing algorithm (Automated)*

##### **Profile Applicability:**

- STIG

##### **Description:**

A cryptographic hash function converts an arbitrary-length input into a fixed length output. Password hashing performs a one-way transformation of a password, turning the password into another string, called the hashed password.

NIST Federal Information Processing Standard (FIPS) 140-2 "Security Requirements for Cryptographic Modules"

Federal Information Processing Standard (140-2) specifies the security requirements that will be satisfied by a cryptographic module, providing four increasing, qualitative levels intended to cover a wide range of potential applications and environments. The areas covered, related to the secure design and implementation of a cryptographic module, include specification; ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

##### **Rationale:**

The **SHA-512** algorithm provides a strong FIPS 140-2 approved hash for password hash generation. A stronger hash provides additional protection to the system by increasing the level of effort needed for an attacker to successfully determine local group passwords.

The operating system must encrypt all stored passwords with a FIPS 140-2 approved cryptographic hashing algorithm.

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and data may be compromised.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DoD requirements.

## Audit:

Run the following script to verify all interactive user accounts passwords are hashed using the **sha512** hashing algorithm:

```
#!/usr/bin/env bash

{
    a_output2=()
    l_valid_shells="^($(awk -F\ / ' $NF != "nologin" {print}' /etc/shells | sed
-rn '/^\ /\ {s,/,\ \ \ \ /,g;p}' | paste -s -d '|' - ))$"
    while IFS= read -r l_user; do
        l_fuser="$(awk -F: ' ($1=="$l_user" && $2 !~ /\^! / && $2 !~
/\^!? \$6 \$/) {print $1}' /etc/shadow)"
        [ -n "$l_fuser" ] && a_output2+=(" - User: \"$l_fuser\" password was
not hashed" \
            " using the sha512 hashing algorithm")
        done < <(awk -v pat="$l_valid_shells" -F: ' ($NF) ~ pat) {print $1}'
/etc/passwd)
        if [ "${#a_output2[@]}" -le 0 ]; then
            printf '%s\n' "" "- Audit Result:" " ** PASS **" \
                " All interactive user's passwords were hashed using the sha512
hashing algorithm" ""
        else
            printf '%s\n' "" "- Audit Result:" " ** FAIL **" " - Reason(s) for
audit failure:" "${a_output2[@]}"
        fi
    }
}
```

## Remediation:

Run the following script to lock all local interactive user accounts with a password that is not using the **sha512** hashing algorithm until the passwords can be regenerated using **sha512**:

```
#!/usr/bin/env bash

{
  a_output2=()
  l_valid_shells="^($(awk -F\| ' $NF != "nologin" {print}' /etc/shells | sed
-rn '/^\|/{s/,,\|\\|/,g;p}' | paste -s -d '|' - ))$"
  while IFS= read -r l_user; do
    while IFS= read -r l_fuser; do
      a_output2+=(" - User: \"$l_fuser\" password was not hashed using
the sha512 hashing algorithm")
      if [ "$l_fuser" = "root" ]; then
        a_output2+=("      The root user needs a new password" \
"      Either create a new password or lock the root account")
      else
        a_output2+=("      * Locking user: \"$l_fuser\"")
        passwd -l "$l_fuser"
      fi
      done < <(awk -F: '($1=="$l_user" && $2 !~ /\^!\/ && $2 !~
/\^!?\$6\$/ ) {print $1}' /etc/shadow)
      done < <(awk -v pat="$l_valid_shells" -F: '($NF) ~ pat) {print $1}'
/etc/passwd)
      if [ "${#a_output2[@]}" -le 0 ]; then
        printf '%s\n' "" " - Remediation complete" "      No remediation
required" ""
      else
        printf '%s\n' "" "${a_output2[@]}" ""
      fi
    fi
  fi
}
```

Ensure all accounts that are locked either have a new password generated using the **SHA512** hashing algorithm

**- OR -**

Ensure the account(s) are removed in accordance with local site account deletion policy  
**Important:** The root account will not be locked by the remediator script. If the Audit returned the root account as requiring an update to it's password hash, please manually update the root account password or lock the root account in accordance with local site policy

## References:

1. NIST SP 800-53 Rev. 5: IA-5
2. NIST SP 800-53 :: IA-5 (1) (c)
3. NIST SP 800-53A :: IA-5 (1).1 (v)
4. NIST FIPS 140-2

## Additional Information:

### Red Hat Enterprise Linux 8

Red Hat Enterprise Linux 8 STIG  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230232  
RULE ID: SV-230232r877397  
STIG ID: RHEL-08-010120  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | IG 1 | IG 2 | IG 3 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.11 <u>Encrypt Sensitive Data at Rest</u></b><br>Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data. |      | ●    | ●    |
| v7               | <b>16.4 <u>Encrypt or Hash all Authentication Credentials</u></b><br>Encrypt or hash with a salt all authentication credentials when stored.                                                                                                                                                                                                                                                                                                                                    |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1003, T1003.008, T1110, T1110.002 | TA0006  | M1041       |



### *5.4.1.10 Ensure temporary accounts have been provisioned with an expiration date of 72 hours (Manual)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Temporary user accounts must be provisioned with an expiration time of 72 hours or less.

#### **Rationale:**

If temporary user accounts remain active when no longer needed or for an excessive period, these accounts may be used to gain unauthorized access. To mitigate this risk, automated termination of all temporary accounts must be set upon account creation.

Temporary accounts are established as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation.

If temporary accounts are used, the operating system must be configured to automatically terminate these types of accounts after a DoD-defined time period of 72 hours.

To address access requirements, many RHEL 8 operating systems may be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

#### **Audit:**

Verify that temporary accounts have been provisioned with an expiration date of 72 hours.

For every existing temporary account, run the following command to obtain its account expiration information.

```
# chage -l system_account_name
```

Verify each of these accounts has an expiration date set within 72 hours.

If any temporary accounts have no expiration date set or do not expire within 72 hours, this is a finding.

## Remediation:

If a temporary account must be created configure the system to terminate the account after a 72 hour time period with the following command to set an expiration date on it. Substitute "system\_account\_name" with the account to be created.

```
# chage -E `date -d "+3 days" +%Y-%m-%d` system_account_name
```

## Additional Information:

```
Red Hat Enterprise Linux 8
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230331
RULE ID: SV-230331r627750
STIG ID: RHEL-08-020000
SEVERITY: CAT II
```

## CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### 5.4.1.11 Ensure fail\_delay is configured (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must enforce a delay of at least four seconds between logon prompts following a failed logon attempt.

#### Rationale:

Configuring the operating system to implement organization-wide security implementation guides and security checklists verifies compliance with federal standards and establishes a common security baseline across the DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

#### Audit:

Verify the operating system enforces a delay of at least four seconds between console logon prompts following a failed logon attempt with the following command:

```
# grep -i fail_delay /etc/login.defs  
FAIL_DELAY 4
```

If the value of "FAIL\_DELAY" is not set to "4" or greater, or the line is commented out, this is a finding.

#### Remediation:

Configure the operating system to enforce a delay of at least four seconds between logon prompts following a failed console logon attempt.

Modify the "/etc/login.defs" file to set the "FAIL\_DELAY" parameter to "4" or greater:

```
FAIL_DELAY 4
```

#### References:

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230378  
Rule ID: SV-230378r627750  
STIG ID: RHEL-08-020310  
Severity: CAT II

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### 5.4.1.12 Ensure pass\_min\_len is configured (Automated)

#### Profile Applicability:

- STIG

#### Description:

Passwords for new users must have a minimum of 15 characters.

#### Rationale:

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to increase exponentially the time and/or resources required to compromise the password.

The DoD minimum password requirement is 15 characters.

#### Audit:

Verify that the operating system enforces a minimum 15-character password length for new user accounts by running the following command:

```
# grep -i pass_min_len /etc/login.defs  
  
PASS_MIN_LEN 15
```

If the "PASS\_MIN\_LEN" parameter value is less than "15", or commented out, this is a finding.

#### Remediation:

Configure operating system to enforce a minimum 15-character password length for new user accounts.

Add, or modify the following line in the "/etc/login.defs" file:

```
PASS_MIN_LEN 15
```

#### References:

1. NIST SP 800-53 :: IA-5 (1) (a)
2. NIST SP 800-53A :: IA-5 (1).1 (i)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230370  
Rule ID: SV-230370r627750  
STIG ID: RHEL-08-020231  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

### *5.4.1.13 Ensure the maximum time period for existing passwords is restricted to 60 days (Automated)*

**Profile Applicability:**

- STIG

**Description:**

User account passwords must be configured so that existing passwords are restricted to a 60-day maximum lifetime.

**Rationale:**

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system's passwords could be compromised.

**Audit:**

Check whether the maximum time period for existing passwords is restricted to 60 days with the following commands:

```
# awk -F: '$5 > 60 {print $1 " " $5}' /etc/shadow
# awk -F: '$5 <= 0 {print $1 " " $5}' /etc/shadow
```

If any results are returned that are not associated with a system account, this is a finding.

**Remediation:**

Configure non-compliant accounts to enforce a 60-day maximum password lifetime restriction.

```
# chage -M 60 [user]
```

**References:**

1. NIST SP 800-53 :: IA-5 (1) (d)
2. NIST SP 800-53A :: IA-5 (1).1 (v)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230367  
Rule ID: SV-230367r627750  
STIG ID: RHEL-08-020210  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |



## **5.4.2 Configure root and system accounts and environment**

### 5.4.2.1 Ensure root is the only UID 0 account (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

Any account with UID 0 has superuser privileges on the system.

#### Rationale:

This access must be limited to only the default **root** account and only from the system console. Administrative access must be through an unprivileged account using an approved mechanism as noted in Item 5.6 Ensure access to the su command is restricted.

#### Audit:

Run the following command and verify that only "root" is returned:

```
# awk -F: '($3 == 0) { print $1 }' /etc/passwd  
root
```

#### Remediation:

Run the following command to change the **root** account UID to **0**:

```
# usermod -u 0 root
```

Modify any users other than **root** with UID **0** and assign them a new UID.

#### References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5
2. NIST SP 800-53A :: CM-6.1 (iv)

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230534  
Rule ID: SV-230534r627750  
STIG ID: RHEL-08-040200  
Severity: CAT II

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1548, T1548.000            | TA0001  | M1026       |

### 5.4.2.2 Ensure root is the only GID 0 account (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The **usermod** command can be used to specify which group the **root** account belongs to. This affects permissions of files that are created by the **root** account.

#### Rationale:

Using GID 0 for the **root** account helps prevent **root** -owned files from accidentally becoming accessible to non-privileged users.

#### Audit:

Run the following command to verify the **root** user's primary GID is 0, and no other user's have GID 0 as their primary GID:

```
# awk -F: '($1 !~ /^(sync|shutdown|halt|operator)/ && $4=="0") {print $1":"$4}' /etc/passwd

root:0
```

**Note:** User's: sync, shutdown, halt, and operator are excluded from the check for other user's with GID 0

#### Remediation:

Run the following command to set the **root** user's GID to 0:

```
# usermod -g 0 root
```

Run the following command to set the **root** group's GID to 0:

```
# groupmod -g 0 root
```

Remove any users other than the **root** user with GID 0 or assign them a new GID if appropriate.

#### References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1548, T1548.000            | TA0005  | M1026       |

### 5.4.2.3 Ensure group root is the only GID 0 group (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The **groupmod** command can be used to specify which group the **root** group belongs to. This affects permissions of files that are group owned by the **root** group.

#### Rationale:

Using GID 0 for the **root** group helps prevent **root** group owned files from accidentally becoming accessible to non-privileged users.

#### Audit:

Run the following command to verify no group other than **root** is assigned GID 0:

```
# awk -F: '$3=="0"{print $1":"$3}' /etc/group  
root:0
```

#### Remediation:

Run the following command to set the **root** group's GID to 0:

```
# groupmod -g 0 root
```

Remove any groups other than the **root** group with GID 0 or assign them a new GID if appropriate.

#### References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1548, T1548.000            | TA0005  | M1026       |

### 5.4.2.4 Ensure root account access is controlled (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

There are a number of methods to access the root account directly. Without a password set any user would be able to gain access and thus control over the entire system.

#### Rationale:

Access to **root** should be secured at all times.

#### Impact:

If there are any automated processes that relies on access to the root account without authentication, they will fail after remediation.

#### Audit:

Run the following command to verify that either the root user's password is set or the root user's account is locked:

```
# passwd -S root | awk '$2 ~ /^(P|L)/ {print "User: \"" $1 "\"" Password is status: " $2}'
```

Verify the output is either:

```
User: "root" Password is status: P
- OR -
User: "root" Password is status: L
```

#### Note:

- **P** - Password is set
- **L** - Password is locked



## Remediation:

Run the following command to set a password for the **root** user:

```
# passwd root
```

- OR -

Run the following command to lock the **root** user account:

```
# usermod -L root
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1078                       | TA0005  | M1026       |

### *5.4.2.5 Ensure root path integrity (Automated)*

**Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

**Description:**

The **root** user can execute any command on the system and could be fooled into executing programs unintentionally if the **PATH** is not set correctly.

**Rationale:**

Including the current working directory (.) or other writable directory in **root**'s executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as **root** to execute a Trojan horse program.

## Audit:

Run the following script to verify root's path does not include:

- Locations that are not directories
- An empty directory (:::)
- A trailing (:)
- Current working directory (.)
- Non **root** owned directories
- Directories that less restrictive than mode **0755**

```
#!/usr/bin/env bash

{
    l_output2=""
    l_pmask="0022"
    l_maxperm="$( printf '%o' $(( 0777 & ~$l_pmask )) )"
    l_root_path="$(sudo -Hiu root env | grep '^PATH' | cut -d= -f2)"
    unset a_path_loc && IFS=":" read -ra a_path_loc <<< "$l_root_path"
    grep -q "::-" <<< "$l_root_path" && l_output2="$l_output2\n - root's path
contains a empty directory (:::)"
    grep -Pq ":\h*$" <<< "$l_root_path" && l_output2="$l_output2\n - root's
path contains a trailing (:)"
    grep -Pq '(\h+|:)\.(:|\h*$)' <<< "$l_root_path" && l_output2="$l_output2\n
- root's path contains current working directory (.)"
    while read -r l_path; do
        if [ -d "$l_path" ]; then
            while read -r l_fmode l_fown; do
                [ "$l_fown" != "root" ] && l_output2="$l_output2\n - Directory:
\"$l_path\" is owned by: \"$l_fown\" should be owned by \"root\""
                [ $(( $l_fmode & $l_pmask )) -gt 0 ] && l_output2="$l_output2\n -
Directory: \"$l_path\" is mode: \"$l_fmode\" and should be mode:
\"$l_maxperm\" or more restrictive"
                done <<< "$(stat -Lc '%#a %U' "$l_path")"
            else
                l_output2="$l_output2\n - \"$l_path\" is not a directory"
            fi
        done <<< "$(printf "%s\n" "${a_path_loc[@]}")"
        if [ -z "$l_output2" ]; then
            echo -e "\n- Audit Result:\n  *** PASS ***\n - Root's path is correctly
configured\n"
        else
            echo -e "\n- Audit Result:\n  ** FAIL **\n - * Reasons for audit
failure * :\n$l_output2\n"
        fi
    }
}
```

## Remediation:

Correct or justify any:

- Locations that are not directories
- Empty directories (::)
- Trailing (:)
- Current working directory (.)
- Non root owned directories
- Directories that less restrictive than mode 0755

## References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1204, T1204.002            | TA0006  | M1022       |

### 5.4.2.6 Ensure root user umask is configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The user file-creation mode mask (**umask**) is used to determine the file permission for newly created directories and files. In Linux, the default permissions for any newly created directory is 0777 (**rw-rw-rw-**), and for any newly created file it is 0666 (**rw-rw-rw-**). The **umask** modifies the default Linux permissions by restricting (masking) these permissions. The **umask** is not simply subtracted, but is processed bitwise. Bits set in the **umask** are cleared in the resulting file mode.

**umask** can be set with either **Octal** or **Symbolic** values:

- **Octal** (Numeric) Value - Represented by either three or four digits. ie **umask 0027** or **umask 027**. If a four digit umask is used, the first digit is ignored. The remaining three digits effect the resulting permissions for user, group, and world/other respectively.
- **Symbolic** Value - Represented by a comma separated list for User **u**, group **g**, and world/other **o**. The permissions listed are not masked by **umask**. ie a **umask** set by **umask u=rwx,g=rx,o=** is the **Symbolic** equivalent of the **Octal umask 027**. This **umask** would set a newly created directory with file mode **drwxr-x---** and a newly created file with file mode **rw-r-----**.

#### root user Shell Configuration Files:

- **/root/.bash\_profile** - Is executed to configure the root users' shell before the initial command prompt. **Is only read by login shells.**
- **/root/.bashrc** - Is executed for interactive shells. **only read by a shell that's both interactive and non-login**

**umask** is set by order of precedence. If **umask** is set in multiple locations, this order of precedence will determine the system's default **umask**.

#### Order of precedence:

1. **/root/.bash\_profile**
2. **/root/.bashrc**
3. The system default umask

Setting a secure value for `umask` ensures that users make a conscious choice about their file permissions. A permissive `umask` value could result in directories or files with excessive permissions that can be read and/or written to by unauthorized users.

Run the following to verify the root user `umask` is set to enforce a newly created directories' permissions to be `750 (drwxr-x---)`, and a newly created file's permissions be `640 (rw-r-----)`, or more restrictive:

### Remediation:

Edit `/root/.bash_profile` and `/root/.bashrc` and remove, comment out, or update any line with `umask` to be `0027` or more restrictive.

System default **umask**

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                          | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <p><b><u>3.3 Configure Data Access Control Lists</u></b></p> <p>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.</p>                                                                                                                                                        |  |  |  |
| v7               | <p><b><u>14.6 Protect Information through Access Control Lists</u></b></p> <p>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.</p> |  |  |  |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1083                              | TA0007         |                    |

### 5.4.2.7 Ensure system accounts do not have a valid login shell (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

There are a number of accounts provided with most distributions that are used to manage applications and are not intended to provide an interactive shell. Furthermore, a user may add special accounts that are not intended to provide an interactive shell.

#### Rationale:

It is important to make sure that accounts that are not being used by regular users are prevented from being used to provide an interactive shell. By default, most distributions set the password field for these accounts to an invalid string, but it is also recommended that the shell field in the password file be set to the **nologin** shell. This prevents the account from potentially being used to run any commands.

#### Audit:

Run the following command to verify system accounts, except for **root**, **halt**, **sync**, **shutdown** or **nfsnobody**, do not have a valid login shell:

```
#!/usr/bin/env bash

{
  l_valid_shells="^($(awk -F\| '$NF != "nologin" {print}' /etc/shells | sed
-rn '/^\\/{s/,/,\\\\/,g;p}' | paste -s -d '|' - ))$"
  awk -v pat="$l_valid_shells" -F:
'($1!~/^(root|halt|sync|shutdown|nfsnobody)$/ && ($3<'$(awk
'/^\\s*UID_MIN/{print $2}' /etc/login.defs)'" || $3 == 65534) && $(NF) ~ pat)
{print "Service account: \"\" $1 \"\" has a valid shell: \" $7}' /etc/passwd
}
```

Nothing should be returned



## Remediation:

Run the following command to set the shell for any service accounts returned by the audit to **nologin**:

```
# usermod -s $(command -v nologin) <user>
```

### Example script:

```
#!/usr/bin/env bash

{
  l_valid_shells="^($( awk -F\| ' $NF != "nologin" {print}' /etc/shells | sed
-rn '/^\\/{s/,/,\\\\/,g;p}' | paste -s -d '|' - ))$"
  awk -v pat="$l_valid_shells" -F:
' ($1!~/^(root|halt|sync|shutdown|nfsnobody)$/ && ($3<'$(awk
'/^\\s*UID_MIN/{print $2}' /etc/login.defs)' || $3 == 65534) && $(NF) ~ pat)
{system ("usermod -s '$(command -v nologin)' " $1)}' /etc/passwd
}
```

## References:

1. NIST SP 800-53 Rev. 5: AC-2(5), AC-3, AC-11, MP-2

## Additional Information:

The **root**, **sync**, **shutdown**, and **halt** users are exempted from requiring a non-login shell.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1078, T1078.001, T1078.003 | TA0005  | M1026       |

### 5.4.2.8 Ensure accounts without a valid login shell are locked (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

There are a number of accounts provided with most distributions that are used to manage applications and are not intended to provide an interactive shell. Furthermore, a user may add special accounts that are not intended to provide an interactive shell.

#### Rationale:

It is important to make sure that accounts that are not being used by regular users are prevented from being used to provide an interactive shell. By default, most distributions set the password field for these accounts to an invalid string, but it is also recommended that the shell field in the password file be set to the **nologin** shell. This prevents the account from potentially being used to run any commands.

#### Audit:

Run the following script to verify all non-root accounts without a valid login shell are locked.

```
#!/usr/bin/env bash

{
  l_valid_shells="^($(awk -F\ / '$NF != "nologin" {print}' /etc/shells | sed
-rn '/^\/\{s,/,,\|\/,g;p}' | paste -s -d '|' - ))$"
  while IFS= read -r l_user; do
    passwd -S "$l_user" | awk '$2 !~ /^L/ {print "Account: \"\" $1 "\" does
not have a valid login shell and is not locked"}'
    done << (awk -v pat="$l_valid_shells" -F: '($1 != "root" && $(NF) !~ pat)
{print $1}' /etc/passwd)
  }
}
```

Nothing should be returned

## Remediation:

Run the following command to lock any non-root accounts without a valid login shell returned by the audit:

```
# usermod -L <user>
```

### Example script:

```
#!/usr/bin/env bash

{
  l_valid_shells="^($(awk -F\ / ' $NF != "nologin" {print}' /etc/shells | sed
-rn '/^\//{s/,/,\\\\/,g;p}' | paste -s -d '|' - ))$"
  while IFS= read -r l_user; do
    passwd -S "$l_user" | awk '$2 !~ /^L/ {system ("usermod -L " $1)}'
  done < <(awk -v pat="$l_valid_shells" -F: '($1 != "root" && $(NF) !~ pat)
{print $1}' /etc/passwd)
}
```

## References:

1. NIST SP 800-53 Rev. 5: AC-2(5), AC-3, AC-11, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 Protect Information through Access Control Lists</b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1078, T1078.001, T1078.003 | TA0005  | M1026       |

### *5.4.2.9 Ensure all accounts on the system are assigned to an active system, application, or user account (Manual)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must not have unnecessary accounts.

#### **Rationale:**

Accounts providing no operational purpose provide additional opportunities for system compromise. Unnecessary accounts include user accounts for individuals not requiring access to the system and application accounts for applications not installed on the system.

#### **Audit:**

Verify all accounts on the system are assigned to an active system, application, or user account.

Obtain the list of authorized system accounts from the Information System Security Officer (ISSO).

Check the system accounts on the system with the following command:

```
# more /etc/passwd

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
```

Accounts such as "games" and "gopher" are not authorized accounts as they do not support authorized system functions.

If the accounts on the system do not match the provided documentation, or accounts that do not support an authorized system function are present, this is a finding.

#### **Remediation:**

Configure the system so all accounts on the system are assigned to an active system, application, or user account.

Remove accounts that do not support approved system activities or that allow for a normal user to perform administrative-level actions.

Document all authorized accounts on the system.

## References:

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230379  
Rule ID: SV-230379r627750  
STIG ID: RHEL-08-020320  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### **5.4.3 Configure user default environment**

### 5.4.3.1 Ensure *nologin* is not listed in */etc/shells* (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

#### Description:

*/etc/shells* is a text file which contains the full pathnames of valid login shells. This file is consulted by *chsh* and available to be queried by other programs.

Be aware that there are programs which consult this file to find out if a user is a normal user; for example, FTP daemons traditionally disallow access to users with shells not included in this file.

#### Rationale:

A user can use *chsh* to change their configured shell.

If a user has a shell configured that isn't in */etc/shells*, then the system assumes that they're somehow restricted. In the case of *chsh* it means that the user cannot change that value.

Other programs might query that list and apply similar restrictions.

By putting *nologin* in */etc/shells*, any user that has *nologin* as its shell is considered a full, unrestricted user. This is not the expected behavior for *nologin*.

#### Audit:

Run the following command to verify that *nologin* is not listed in the */etc/shells* file:

```
# grep -Ps '^h*([^\n\r]+)?\/nologin\b' /etc/shells
```

Nothing should be returned

#### Remediation:

Edit */etc/shells* and remove any lines that include *nologin*

#### References:

1. shells(5)
2. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5



### 5.4.3.2 Ensure default user shell timeout is configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

**TMOUT** is an environmental setting that determines the timeout of a shell in seconds.

- **TMOUT=*n*** - Sets the shell timeout to *n* seconds. A setting of **TMOUT=0** disables timeout.
- **readonly TMOUT** - Sets the TMOUT environmental variable as readonly, preventing unwanted modification during run-time.
- **export TMOUT** - exports the TMOUT variable

#### System Wide Shell Configuration Files:

- **/etc/profile** - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in the **.bash\_profile**, however this file is used to set an initial PATH or PS1 for all shell users of the system. **is only executed for interactive login shells, or shells executed with the --login parameter.**
- **/etc/profile.d** - **/etc/profile** will execute the scripts within **/etc/profile.d/\*.sh**. It is recommended to place your configuration in a shell script within **/etc/profile.d** to set your own system wide environmental variables.
- **/etc/bashrc** - System wide version of **.bashrc**. In Fedora derived distributions, **/etc/bashrc** also invokes **/etc/profile.d/\*.sh** if *non-login* shell, but redirects output to **/dev/null** if *non-interactive*. **Is only executed for interactive shells or if BASH\_ENV is set to /etc/bashrc.**

#### Rationale:

Setting a timeout value reduces the window of opportunity for unauthorized user access to another user's shell session that has been left unattended. It also ends the inactive session and releases the resources associated with that session.

## Audit:

Run the following script to verify that **TMOUT** is configured to: include a timeout of no more than **900** seconds, to be **readonly**, to be **exported**, and is not being changed to a longer timeout.

```
#!/usr/bin/env bash

{
    output1="" output2=""
    [ -f /etc/bashrc ] && BRC="/etc/bashrc"
    for f in "$BRC" /etc/profile /etc/profile.d/*.sh ; do
        grep -Pq '^s*([^\#]+\s+)?TMOUT=(900|[1-8][0-9][0-9]|[1-9][0-9]|[1-9])\b' "$f" && grep -Pq
'^s*([^\#]+\s+)?readonly\s+TMOUT(\s+|\s*;\s*$|=(900|[1-8][0-9][0-9]|[1-9][0-9]|[1-9]))\b' "$f" && grep -Pq
'^s*([^\#]+\s+)?export\s+TMOUT(\s+|\s*;\s*$|=(900|[1-8][0-9][0-9]|[1-9][0-9]|[1-9]))\b' "$f" &&
        output1="$f"
    done
    grep -Pq '^s*([^\#]+\s+)?TMOUT=(9[0-9][1-9]|9[1-9][0-9]|0+|[1-9]\d{3,})\b'
/etc/profile /etc/profile.d/*.sh "$BRC" && output2=$(grep -Ps
'^s*([^\#]+\s+)?TMOUT=(9[0-9][1-9]|9[1-9][0-9]|0+|[1-9]\d{3,})\b'
/etc/profile /etc/profile.d/*.sh $BRC)
    if [ -n "$output1" ] && [ -z "$output2" ]; then
        echo -e "\nPASSED\n\nTMOUT is configured in: \"$output1\"\n"
    else
        [ -z "$output1" ] && echo -e "\nFAILED\n\nTMOUT is not configured\n"
        [ -n "$output2" ] && echo -e "\nFAILED\n\nTMOUT is incorrectly
configured in: \"$output2\"\n"
    fi
}
```

## Remediation:

Review `/etc/bashrc`, `/etc/profile`, and all files ending in `*.sh` in the `/etc/profile.d/` directory and remove or edit all `TMOUT=_n_` entries to follow local site policy. `TMOUT` should not exceed 900 or be equal to 0.

Configure `TMOUT` in **one** of the following files:

- A file in the `/etc/profile.d/` directory ending in `.sh`
- `/etc/profile`
- `/etc/bashrc`

### *TMOUT configuration examples:*

- As multiple lines:

```
TMOUT=900
readonly TMOUT
export TMOUT
```

- As a single line:

```
readonly TMOUT=900 ; export TMOUT
```

## Additional Information:

The audit and remediation in this recommendation apply to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked. Other methods of setting a timeout exist for other shells not covered here.

Ensure that the timeout conforms to your local policy.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.3 Configure Automatic Session Locking on Enterprise Assets</b><br>Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. |  |  |  |
| v7               | <b>16.11 Lock Workstation Sessions After Inactivity</b><br>Automatically lock workstation sessions after a standard period of inactivity.                                                                                                                                                                              |  |  |  |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1078                              | TA0005         | M1026              |

### 5.4.3.3 Ensure default user umask is configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The user file-creation mode mask (**umask**) is used to determine the file permission for newly created directories and files. In Linux, the default permissions for any newly created directory is 0777 (**rxwxrwxrwx**), and for any newly created file it is 0666 (**rw-rw-rw-**). The **umask** modifies the default Linux permissions by restricting (masking) these permissions. The **umask** is not simply subtracted, but is processed bitwise. Bits set in the **umask** are cleared in the resulting file mode.

**umask** can be set with either **Octal** or **Symbolic** values:

- **Octal** (Numeric) Value - Represented by either three or four digits. ie **umask 0027** or **umask 027**. If a four digit umask is used, the first digit is ignored. The remaining three digits effect the resulting permissions for user, group, and world/other respectively.
- **Symbolic** Value - Represented by a comma separated list for User **u**, group **g**, and world/other **o**. The permissions listed are not masked by **umask**. ie a **umask** set by **umask u=rwx,g=rx,o=** is the **Symbolic** equivalent of the **Octal umask 027**. This **umask** would set a newly created directory with file mode **drwxr-x---** and a newly created file with file mode **rw-r-----**.

The default **umask** can be set to use the **pam\_umask** module or in a **System Wide Shell Configuration File**. The user creating the directories or files has the discretion of changing the permissions via the **chmod** command, or choosing a different default **umask** by adding the **umask** command into a **User Shell Configuration File**, ( **.bash\_profile** or **.bashrc**), in their home directory.

## Setting the default umask:

- pam\_umask module:
  - will set the umask according to the system default in `/etc/login.defs` and user settings, solving the problem of different `umask` settings with different shells, display managers, remote sessions etc.
  - `umask=<mask>` value in the `/etc/login.defs` file is interpreted as Octal
  - Setting `USERGROUPS_ENAB` to yes in `/etc/login.defs` (default):
    - will enable setting of the `umask` group bits to be the same as owner bits. (examples: 022 -> 002, 077 -> 007) for non-root users, if the `uid` is the same as `gid`, and `username` is the same as the `<primary group name>`
    - `userdel` will remove the user's group if it contains no more members, and `useradd` will create by default a group with the name of the user
- System Wide Shell Configuration File:
  - `/etc/profile` - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in the `.bash_profile`, however this file is used to set an initial PATH or PS1 for all shell users of the system. **is only executed for interactive login shells, or shells executed with the `--login` parameter.**
  - `/etc/profile.d` - `/etc/profile` will execute the scripts within `/etc/profile.d/*.sh`. It is recommended to place your configuration in a shell script within `/etc/profile.d` to set your own system wide environmental variables.
  - `/etc/bashrc` - System wide version of `.bashrc`. In Fedora derived distributions, `etc/bashrc` also invokes `/etc/profile.d/*.sh` if *non-login* shell, but redirects output to `/dev/null` if *non-interactive*. **Is only executed for interactive shells or if `BASH_ENV` is set to `/etc/bashrc`.**

## User Shell Configuration Files:

- `~/.bash_profile` - Is executed to configure your shell before the initial command prompt. **Is only read by login shells.**
- `~/.bashrc` - Is executed for interactive shells. **only read by a shell that's both interactive and non-login**

`umask` is set by order of precedence. If `umask` is set in multiple locations, this order of precedence will determine the system's default `umask`.

**Order of precedence:**

1. A file in `/etc/profile.d/` ending in `.sh` - This will override any other system-wide `umask` setting
2. In the file `/etc/profile`
3. On the `pam_umask.so` module in `/etc/pam.d/postlogin`
4. In the file `/etc/login.defs`
5. In the file `/etc/default/login`

**Rationale:**

Setting a secure default value for `umask` ensures that users make a conscious choice about their file permissions. A permissive `umask` value could result in directories or files with excessive permissions that can be read and/or written to by unauthorized users.

## Audit:

Run the following to verify the default user **umask** is set to **027**(octal) or **u=rwx,g=rx,o=** (Symbolic) to enforce newly created directories' permissions to be **750** (**drwxr-x---**), and newly created file's permissions be **640** (**rw-r-----**), or more restrictive:

```
#!/usr/bin/env bash

{
    l_output="" l_output2=""
    file_umask_chk()
    {
        if grep -Pseq -- '^\\h*umask\\h+(0?[0-7][2-7]7|u(=[rwx]{0,3}),g(=[rx]{0,2}),o(=[h*#.]*)?\\$' "$l_file"; then
            l_output="$l_output\\n - umask is set correctly in \"$l_file\\n\"
            elif grep -Pseq -- '^\\h*umask\\h+(((0-7)[0-7][01][0-7]\\b|[0-7][0-7][0-7][0-6]\\b)|((0-7)[01][0-7]\\b|[0-7][0-7][0-6]\\b)|(u(=[rwx]{1,3}),)?((g(=[rx]?[rx]?w[rx]?[rx]?\\b)(,o(=[rwx]{1,3}))?)|((g(=[wrx]{1,3}),)?o(=[wrx]{1,3}\\b))))' "$l_file"; then
                l_output2="$l_output2\\n - umask is incorrectly set in \"$l_file\\n\"
            fi
        }
        while IFS= read -r -d $'\\0' l_file; do
            file_umask_chk
            done <<(find /etc/profile.d/ -type f -name '*.sh' -print0)
            [ -z "$l_output" ] && l_file="/etc/profile" && file_umask_chk
            [ -z "$l_output" ] && l_file="/etc/bashrc" && file_umask_chk
            [ -z "$l_output" ] && l_file="/etc/bash.bashrc" && file_umask_chk
            [ -z "$l_output" ] && l_file="/etc/pam.d/postlogin"
            if [ -z "$l_output" ]; then
                if grep -Pseq -- '^\\h*session\\h+([#\\n\\r]+\\h+pam_umask\\.so\\h+([#\\n\\r]+\\h+)?umask=(0?[0-7][2-7]7)\\b' "$l_file"; then
                    l_output1="$l_output1\\n - umask is set correctly in \"$l_file\\n\"
                    elif grep -Pseq '^\\h*session\\h+([#\\n\\r]+\\h+pam_umask\\.so\\h+([#\\n\\r]+\\h+)?umask=((0-7)[0-7][01][0-7]\\b|[0-7][0-7][0-7][0-6]\\b)|((0-7)[01][0-7]\\b))' "$l_file"; then
                        l_output2="$l_output2\\n - umask is incorrectly set in \"$l_file\\n\"
                    fi
                fi
                [ -z "$l_output" ] && l_file="/etc/login.defs" && file_umask_chk
                [ -z "$l_output" ] && l_file="/etc/default/login" && file_umask_chk
                [[ -z "$l_output" && -z "$l_output2" ]] && l_output2="$l_output2\\n - umask is not set"
                if [ -z "$l_output2" ]; then
                    echo -e "\\n- Audit Result:\\n  ** PASS **\\n - * Correctly configured * :\\n$l_output\\n"
                else
                    echo -e "\\n- Audit Result:\\n  ** FAIL **\\n - * Reasons for audit failure * :\\n$l_output2"
                    [ -n "$l_output" ] && echo -e "\\n- * Correctly configured * :\\n$l_output\\n"
                fi
            }
}
```



Run the following script and perform the instructions in the output to set the default umask to **027** or more restrictive:

Page 1172

## Notes:

- This method only applies to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked
- If the `pam_umask.so` module is going to be used to set `umask`, ensure that it's not being overridden by another setting. Refer to the `PAM_UMASK(8)` man page for more information

## Default Value:

UMASK 022

## References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## Additional Information:

- Other methods of setting a default user umask exist
- If other methods are in use in your environment they should be audited
- The default user umask can be overridden with a user specific umask
- The user creating the directories or files has the discretion of changing the permissions:
  - Using the `chmod` command
  - Setting a different default umask by adding the `umask` command into a User Shell Configuration File, (`.bashrc`), in their home directory
  - Manually changing the umask for the duration of a login session by running the `umask` command

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1083                       | TA0007  |             |

#### *5.4.3.4 Ensure emergency accounts have been provisioned with an expiration date of 72 hours (Manual)*

##### **Profile Applicability:**

- STIG

##### **Description:**

Emergency accounts must be automatically removed or disabled after the crisis is resolved or within 72 hours.

##### **Rationale:**

Emergency accounts are privileged accounts established in response to crisis situations where the need for rapid account activation is required. Therefore, emergency account activation may bypass normal account authorization processes. If these accounts are automatically disabled, system maintenance during emergencies may not be possible, thus adversely affecting system availability.

Emergency accounts are different from infrequently used accounts (i.e., local logon accounts used by the organization's system administrators when network or normal logon/access is not available). Infrequently used accounts are not subject to automatic termination dates. Emergency accounts are accounts created in response to crisis situations, usually for use by maintenance personnel. The automatic expiration or disabling time period may be extended as needed until the crisis is resolved; however, it must not be extended indefinitely. A permanent account should be established for privileged users who need long-term maintenance accounts.

To address access requirements, many RHEL operating systems can be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

##### **Audit:**

Verify emergency accounts have been provisioned with an expiration date of 72 hours. For every existing emergency account, run the following command to obtain its account expiration information.

```
# chage -l <temporary_account_name> | grep -i "account expires"
```

Verify each of these accounts has an expiration date set within 72 hours.

If any emergency accounts have no expiration date set or do not expire within 72 hours, this is a finding.

**Remediation:**

If an emergency account must be created, configure the system to terminate the account after 72 hours with the following command to set an expiration date for the account. Substitute <temporary\_account\_name> with the account to be created.

```
# chage -E $(date -d +3days +%Y-%m-%d) <temporary_account_name>
```

The automatic expiration or disabling time period may be extended as needed until the crisis is resolved.

**References:**

- 1. NIST SP 800-53 Revision 5 :: AC-2 (2)
- 2. NIST SP 800-53A :: AC-2 (2).1 (ii)

**Additional Information:**

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024  
  
Vul ID: V-230374  
Rule ID: SV-230374r903129  
STIG ID: RHEL-08-020270  
Severity: CAT II

**CIS Controls:**

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### *5.4.3.5 Ensure the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Account identifiers (individuals, groups, roles, and devices) must be disabled after 35 days of inactivity.

#### **Rationale:**

Inactive identifiers pose a risk to systems and applications because attackers may exploit an inactive identifier and potentially obtain undetected access to the system. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

The operating system needs to track periods of inactivity and disable application identifiers after 35 days of inactivity.

#### **Audit:**

Verify the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity with the following command:

Check the account inactivity value by performing the following command:

```
# grep -i inactive /etc/default/useradd  
  
INACTIVE=35
```

If "INACTIVE" is set to "-1", a value greater than "35", or is commented out, this is a finding.

#### **Remediation:**

Configure the operating system to disable account identifiers after 35 days of inactivity after the password expiration.

Run the following command to change the configuration for useradd:

```
# useradd -D -f 35
```

DoD recommendation is 35 days, but a lower value is acceptable. The value "-1" will disable this feature, and "0" will disable the account immediately after the password expires.

#### **References:**

1. NIST SP 800-53A :: IA-4.1 (iii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230373  
Rule ID: SV-230373r627750  
STIG ID: RHEL-08-020260  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                      | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>4.1 <u>Establish and Maintain a Secure Configuration Process</u></b><br>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | ●    | ●    | ●    |
| v7               | <b>16.9 <u>Disable Dormant Accounts</u></b><br>Automatically disable dormant accounts after a set period of inactivity.                                                                                                                                                                                                                                                                                                      | ●    | ●    | ●    |

### *5.4.3.6 Ensure the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must define default permissions for all authenticated users in such a way that the user can only read and modify their own files.

#### **Rationale:**

Setting the most restrictive default permissions ensures that when new accounts are created, they do not have unnecessary access.

#### **Audit:**

Setting the most restrictive default permissions ensures that when new accounts are created, they do not have unnecessary access.

Check Text: Verify the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files.

Check for the value of the "UMASK" parameter in "/etc/login.defs" file with the following command:

Note: If the value of the "UMASK" parameter is set to "000" in "/etc/login.defs" file, the Severity is raised to a CAT I.

```
# grep -i umask /etc/login.defs
UMASK 077
```

If the value for the "UMASK" parameter is not "077", or the "UMASK" parameter is missing or is commented out, this is a finding.

#### **Remediation:**

Configure the operating system to define default permissions for all authenticated users in such a way that the user can only read and modify their own files.

Add or edit the line for the "UMASK" parameter in "/etc/login.defs" file to "077":

```
UMASK 077
```

#### **References:**

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230383  
Rule ID: SV-230383r627750  
STIG ID: RHEL-08-020351  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### *5.4.3.7 Ensure the operating system enforces a 60-day maximum password lifetime for new user accounts (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

User account passwords must have a 60-day maximum password lifetime restriction.

#### **Rationale:**

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system's passwords could be compromised.

#### **Audit:**

Verify that the operating system enforces a 60-day maximum password lifetime for new user accounts by running the following command:

```
# grep -i pass_max_days /etc/login.defs  
  
PASS_MAX_DAYS 60
```

If the "PASS\_MAX\_DAYS" parameter value is greater than "60", or commented out, this is a finding.

#### **Remediation:**

Configure the operating system to enforce a 60-day maximum password lifetime. Add, or modify the following line in the "/etc/login.defs" file:

```
PASS_MAX_DAYS 60
```

#### **References:**

1. NIST SP 800-53A :: IA-5 (1).1 (v)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230366  
Rule ID: SV-230366r646878  
STIG ID: RHEL-08-020200  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>4.1 Establish and Maintain a Secure Configuration Process</b><br>Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                                                                                                                                                                                           |                                                                                     |  |  |

### 5.4.3.8 Ensure the umask default for installed shells is "077" (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system must define default permissions for logon and non-logon shells.

#### Rationale:

The umask controls the default access mode assigned to newly created files. A umask of 077 limits new files to mode 600 or less permissive. Although umask can be represented as a four-digit number, the first digit representing special access modes is typically ignored or required to be "0". This requirement applies to the globally configured system defaults and the local interactive user defaults for each account on the system.

#### Audit:

Verify that the umask default for installed shells is "077".

Check for the value of the "UMASK" parameter in the "/etc/bashrc", "/etc/csh.cshrc" and "/etc/profile" files with the following command:

Note: If the value of the "UMASK" parameter is set to "000" in either the "/etc/bashrc" the "/etc/csh.cshrc" or the "/etc/profile" files, the Severity is raised to a CAT I.

```
# grep -i umask /etc/bashrc /etc/csh.cshrc /etc/profile

/etc/bashrc: umask 077
/etc/bashrc: umask 077
/etc/csh.cshrc: umask 077
/etc/csh.cshrc: umask 077
/etc/profile:      umask 077
/etc/profile:      umask 077
```

If the value for the "UMASK" parameter is not "077", or the "UMASK" parameter is missing or is commented out, this is a finding.

## Remediation:

Configure the operating system to define default permissions for all authenticated users in such a way that the user can only read and modify their own files.  
Add or edit the lines for the "UMASK" parameter in the "/etc/bashrc" and "/etc/csh.cshrc" and "/etc/profile" files to "077":

UMASK 077

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230385  
Rule ID: SV-230385r792902  
STIG ID: RHEL-08-020353  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### 5.4.3.9 Ensure the default umask for all local interactive users is "077" (Manual)

#### Profile Applicability:

- STIG

#### Description:

The operating system must set the umask value to 077 for all local interactive user accounts.

#### Rationale:

The umask controls the default access mode assigned to newly created files. A umask of 077 limits new files to mode 600 or less permissive. Although umask can be represented as a four-digit number, the first digit representing special access modes is typically ignored or required to be "0". This requirement applies to the globally configured system defaults and the local interactive user defaults for each account on the system.

#### Audit:

Verify that the default umask for all local interactive users is "077".

Identify the locations of all local interactive user home directories by looking at the "/etc/passwd" file.

Check all local interactive user initialization files for interactive users with the following command:

Note: The example is for a system that is configured to create users home directories in the "/home" directory.

```
# grep -ir ^umask /home | grep -v '.bash_history'
```

If any local interactive user initialization files are found to have a umask statement that has a value less restrictive than "077", this is a finding.

#### Remediation:

Remove the umask statement from all local interactive user's initialization files.

If the account is for an application, the requirement for a umask less restrictive than "077" can be documented with the Information System Security Officer, but the user agreement for access to the account must specify that the local interactive user must log on to their account first and then switch the user to the application account with the correct option to gain the account's environment variables.

#### References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230384  
Rule ID: SV-230384r858732  
STIG ID: RHEL-08-020352  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### *5.4.3.10 Ensure the operating system initiates a session lock after 15 minutes of inactivity (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must automatically lock command line user sessions after 15 minutes of inactivity.

#### **Rationale:**

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Satisfies: SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012

#### **Audit:**

Verify the operating system initiates a session lock after 15 minutes of inactivity. Check the value of the system inactivity timeout with the following command:

```
# grep -i lock-after-time /etc/tmux.conf  
  
set -g lock-after-time 900
```

If "lock-after-time" is not set to "900" or less in the global tmux configuration file to enforce session lock after inactivity, this is a finding.

#### **Remediation:**

Configure the operating system to enforce session lock after a period of 15 minutes of inactivity by adding the following line to the "/etc/tmux.conf" global configuration file:

```
set -g lock-after-time 900
```



## References:

1. NIST SP 800-53 :: AC-11 a
2. NIST SP 800-53A :: AC-11.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230353  
Rule ID: SV-230353r627750  
STIG ID: RHEL-08-020070  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u></b><br>Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.                                                                                                                                                                                         |    |    |    |
| v8               | <b>4.10 <u>Enforce Automatic Device Lockout on Portable End-User Devices</u></b><br>Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts. |                                                                                       |  |  |
| v7               | <b>16.11 <u>Lock Workstation Sessions After Inactivity</u></b><br>Automatically lock workstation sessions after a standard period of inactivity.                                                                                                                                                                                                                                                                                                                                                                      |  |  |  |

### *5.4.3.11 Ensure the operating system prevents users from disabling the tmux terminal multiplexer (Automated)*

**Profile Applicability:**

- STIG

**Description:**

The operating system must prevent users from disabling session control mechanisms.

**Rationale:**

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined. Rather than be forced to wait for a period of time to expire before the user session can be locked, the operating system needs to provide users with the ability to manually invoke a session lock so users can secure their session if it is necessary to temporarily vacate the immediate physical vicinity.

Tmux is a terminal multiplexer that enables a number of terminals to be created, accessed, and controlled from a single screen. Red Hat endorses tmux as the recommended session controlling package.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

**Audit:**

Verify the operating system prevents users from disabling the tmux terminal multiplexer with the following command:

```
# grep -i tmux /etc/shells
```

If any output is produced, this is a finding.

**Remediation:**

Configure the operating system to prevent users from disabling the tmux terminal multiplexer by editing the "/etc/shells" configuration file to remove any instances of tmux.

**References:**

1. NIST SP 800-53 :: AC-11 b
2. NIST SP 800-53A :: AC-11.1 (iii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230350  
Rule ID: SV-230350r627750  
STIG ID: RHEL-08-020042  
Severity: CAT III

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u></b><br>Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.                                                                                                                                                                                         |    |    |    |
| v8               | <b>4.10 <u>Enforce Automatic Device Lockout on Portable End-User Devices</u></b><br>Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts. |                                                                                       |   |   |
| v7               | <b>16.11 <u>Lock Workstation Sessions After Inactivity</u></b><br>Automatically lock workstation sessions after a standard period of inactivity.                                                                                                                                                                                                                                                                                                                                                                      |  |  |  |

### *5.4.3.12 Ensure the operating system's shell initialization file is configured to start each shell with the tmux terminal multiplexer (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must ensure session control is automatically started at shell initialization.

#### **Rationale:**

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined. Rather than be forced to wait for a period of time to expire before the user session can be locked, the operating system needs to provide users with the ability to manually invoke a session lock so users can secure their session if it is necessary to temporarily vacate the immediate physical vicinity.

Tmux is a terminal multiplexer that enables a number of terminals to be created, accessed, and controlled from a single screen. Red Hat endorses tmux as the recommended session controlling package.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

## Audit:

Verify the operating system shell initialization file is configured to start each shell with the tmux terminal multiplexer with the following command:

Determine if tmux is currently running:

```
# ps all | grep tmux | grep -v grep
```

If the command does not produce output, this is a finding.

Determine the location of the tmux script:

```
# grep -r tmux /etc/bashrc /etc/profile.d
/etc/profile.d/tmux.sh: case "$name" in (sshd|login) tmux ;; esac
```

Review the tmux script by using the following example:

```
# cat /etc/profile.d/tmux.sh

if [ "$PS1" ]; then
parent=$(ps -o ppid= -p $$)
name=$(ps -o comm= -p $parent)
case "$name" in (sshd|login) tmux ;; esac
fi
```

If "tmux" is not configured as the example above, is commented out, or is missing, this is a finding.

## Remediation:

Configure the operating system to initialize the tmux terminal multiplexer as each shell is called by adding the following line to the end of the "/etc/bashrc" configuration file:

```
if [ "$PS1" ]; then
parent=$(ps -o ppid= -p $$)
name=$(ps -o comm= -p $parent)
case "$name" in (sshd|login) tmux ;; esac
fi
```

This setting will take effect at next logon.

## References:

1. NIST SP 800-53 :: AC-11 b
2. NIST SP 800-53A :: AC-11.1 (iii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230349  
Rule ID: SV-230349r917920  
STIG ID: RHEL-08-020041  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u></b><br>Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.                                                                                                                                                                                         |    |    |    |
| v8               | <b>4.10 <u>Enforce Automatic Device Lockout on Portable End-User Devices</u></b><br>Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts. |                                                                                       |   |   |
| v7               | <b>16.11 <u>Lock Workstation Sessions After Inactivity</u></b><br>Automatically lock workstation sessions after a standard period of inactivity.                                                                                                                                                                                                                                                                                                                                                                      |  |  |  |

### 5.4.3.13 *Ensure the operating system enables the user to initiate a session lock (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures for command line sessions.

#### **Rationale:**

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined. Rather than be forced to wait for a period of time to expire before the user session can be locked, the operating system needs to provide users with the ability to manually invoke a session lock so users can secure their session if it is necessary to temporarily vacate the immediate physical vicinity.

Tmux is a terminal multiplexer that enables a number of terminals to be created, accessed, and controlled from a single screen. Red Hat endorses tmux as the recommended session controlling package.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

#### **Audit:**

Verify the operating system enables the user to initiate a session lock with the following command:

```
# grep -Ei lock-command|lock-session' /etc/tmux.conf  
  
set -g lock-command vlock  
bind X lock-session
```

If the "lock-command" is not set in the global settings to call "vlock", this is a finding.

## Remediation:

Configure the operating system to enable a user to initiate a session lock via tmux. Create a global configuration file "/etc/tmux.conf" and add the following line:

```
set -g lock-command vlock
```

Reload tmux configuration to take effect. This can be performed in tmux while it is running:

```
# tmux source-file /etc/tmux.conf
```

## References:

1. NIST SP 800-53 :: AC-11 b
2. NIST SP 800-53A :: AC-11.1 (iii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230348  
Rule ID: SV-230348r902725  
STIG ID: RHEL-08-020040  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u></b><br>Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.                                                                                                                                                                                         |  |  |  |
| v8               | <b>4.10 <u>Enforce Automatic Device Lockout on Portable End-User Devices</u></b><br>Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts. |                                                                                       |  |  |
| v7               | <b>16.11 <u>Lock Workstation Sessions After Inactivity</u></b><br>Automatically lock workstation sessions after a standard period of inactivity.                                                                                                                                                                                                                                                                                                                                                                      |  |  |  |



### 5.4.3.14 *Ensure the number of concurrent sessions is configured (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must limit the number of concurrent sessions to ten for all accounts and/or account types.

#### **Rationale:**

Operating system management includes the ability to control the number of users and user sessions that utilize an operating system. Limiting the number of allowed users and sessions per user is helpful in reducing the risks related to DoS attacks.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based on mission needs and the operational environment for each system.

#### **Audit:**

Verify the operating system limits the number of concurrent sessions to "10" for all accounts and/or account types by issuing the following command:

```
# grep -r -s '^[^#].*maxlogins' /etc/security/limits.conf  
/etc/security/limits.d/*.conf  
  
* hard maxlogins 10
```

This can be set as a global domain (with the \* wildcard) but may be set differently for multiple domains.

If the "maxlogins" item is missing, commented out, or the value is set greater than "10" and is not documented with the Information System Security Officer (ISSO) as an operational requirement for all domains that have the "maxlogins" item assigned, this is a finding.

## Remediation:

Configure the operating system to limit the number of concurrent sessions to "10" for all accounts and/or account types.

Add the following line to the top of the "/etc/security/limits.conf" or in a ".conf" file defined in "/etc/security/limits.d/":

```
* hard maxlogins 10
```

## References:

1. NIST SP 800-53 :: AC-10
2. NIST SP 800-53A :: AC-10.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230346  
Rule ID: SV-230346r877399  
STIG ID: RHEL-08-020024  
Severity: CAT III

## CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### 5.4.3.15 *Ensure all local interactive users are assigned a home directory upon creation (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

All local interactive user accounts must be assigned a home directory upon creation.

#### **Rationale:**

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

#### **Audit:**

Verify all local interactive users are assigned a home directory upon creation with the following command:

```
# grep -i create_home /etc/login.defs  
  
CREATE_HOME yes
```

If the value for "CREATE\_HOME" parameter is not set to "yes", the line is missing, or the line is commented out, this is a finding.

#### **Remediation:**

Configure the operating system to assign home directories to all new local interactive users by setting the "CREATE\_HOME" parameter in "/etc/login.defs" to "yes" as follows.

```
CREATE_HOME yes
```

#### **References:**

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230324  
Rule ID: SV-230324r627750  
STIG ID: RHEL-08-010760  
Severity: CAT II

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### 5.4.3.16 Ensure StopIdleSessionSec is configured (Automated)

#### Profile Applicability:

- STIG

#### Description:

The Operating System (OS) must terminate idle user sessions.

#### Rationale:

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended.

#### Audit:

Verify that RHEL 8 logs out sessions that are idle for 15 minutes with the following command:

```
# grep -i ^StopIdleSessionSec /etc/systemd/logind.conf  
StopIdleSessionSec=900
```

If "StopIdleSessionSec" is not configured to "900" seconds, this is a finding.

#### Remediation:

Configure RHEL 8 to log out idle sessions by editing the /etc/systemd/logind.conf file with the following line:

```
StopIdleSessionSec=900
```

The "logind" service must be restarted for the changes to take effect. To restart the "logind" service, run the following command:

```
# systemctl restart systemd-logind
```

**Note:** To preserve running user programs such as tmux, uncomment and/or edit "KillUserProcesses=no" in "/etc/systemd/logind.conf".

#### References:

1. NIST SP 800-53 :: SC-10
2. NIST SP 800-53A :: SC-10.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-257258  
RULE ID: SV-257258r942953  
STIG ID: RHEL-08-020035  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u></b><br>Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.                                                                                                                                                                                         |    |    |    |
| v8               | <b>4.10 <u>Enforce Automatic Device Lockout on Portable End-User Devices</u></b><br>Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts. |                                                                                       |   |   |
| v7               | <b>16.11 <u>Lock Workstation Sessions After Inactivity</u></b><br>Automatically lock workstation sessions after a standard period of inactivity.                                                                                                                                                                                                                                                                                                                                                                      |  |  |  |

## 6 Logging and Auditing

The items in this section describe how to configure logging, log monitoring, and auditing, using tools included in most distributions.

It is recommended that `rsyslog` be used for logging (with `logwatch` providing summarization) and `auditd` be used for auditing (with `aureport` providing summarization) to automatically monitor logs for intrusion attempts and other suspicious system behavior.

In addition to the local log files created by the steps in this section, it is also recommended that sites collect copies of their system logs on a secure, centralized log server via an encrypted connection. Not only does centralized logging help sites correlate events that may be occurring on multiple systems, but having a second copy of the system log information may be critical after a system compromise where the attacker has modified the local log files on the affected system(s). If a log correlation system is deployed, configure it to process the logs described in this section.

Because it is often necessary to correlate log information from many different systems (particularly after a security incident) it is recommended that the time be synchronized among systems and devices connected to the local network. The standard Internet protocol for time synchronization is the Network Time Protocol (NTP), which is supported by most network-ready devices. Reference <<http://chrony.tuxfamily.org/>> manual page for more information on configuring chrony.

It is important that all logs described in this section be monitored on a regular basis and correlated to determine trends. A seemingly innocuous entry in one log could be more significant when compared to an entry in another log.

**Note on log file permissions:** There really isn't a "one size fits all" solution to the permissions on log files. Many sites utilize group permissions so that administrators who are in a defined security group, such as "wheel" do not have to elevate privileges to root in order to read log files. Also, if a third party log aggregation tool is used, it may need to have group permissions to read the log files, which is preferable to having it run setuid to root. Therefore, there are two remediation and audit steps for log file permissions. One is for systems that do not have a secured group method implemented that only permits root to read the log files (`root:root 600`). The other is for sites that do have such a setup and are designated as `root:securegrp 640` where `securegrp` is the defined security group (in some cases `wheel`).

## 6.1 Configure Integrity Checking

AIDE is a file integrity checking tool. While it cannot prevent intrusions, it can detect unauthorized changes to configuration files by alerting when the files are changed. When setting up AIDE, decide internally what the site policy will be concerning integrity checking. Review the AIDE quick start guide and AIDE documentation before proceeding.

**Note: - IF -** another local site approved solution is used, and configured to provide the capabilities covered by AIDE in this section, this section may be skipped.



### 6.1.1 Ensure AIDE is installed (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

Advanced Intrusion Detection Environment (AIDE) is a intrusion detection tool that uses predefined rules to check the integrity of files and directories in the Linux operating system. AIDE has its own database to check the integrity of files and directories.

**aide** takes a snapshot of files and directories including modification times, permissions, and file hashes which can then be used to compare against the current state of the filesystem to detect modifications to the system.

#### Rationale:

By monitoring the filesystem state compromised files can be detected to prevent or limit the exposure of accidental or malicious misconfigurations or modified binaries.

#### Audit:

Run the following command and verify **aide** is installed:

```
# rpm -q aide  
aide-<version>
```

#### Remediation:

Run the following command to install **aide**:

```
# dnf install aide
```

Configure **aide** as appropriate for your environment. Consult the **aide** documentation for options.

Initialize **aide**:

Run the following commands:

```
# aide --init  
# mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

#### References:

1. AIDE stable manual: <http://aide.sourceforge.net/stable/manual.html>
2. NIST SP 800-53 Revision 5 :: SI-6 a

## Additional Information:

The prelinking feature can interfere with **aide** because it alters binaries to speed up their start up times. Run **prelink -ua** to restore the binaries to their prelinked state, thus avoiding false positives from **aide**.

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-251710  
Rule ID: SV-251710r880730  
STIG ID: RHEL-08-010359  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                         | IG 1 | IG 2 | IG 3 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.14 <u>Log Sensitive Data Access</u></b><br>Log sensitive data access, including modification and disposal.                                                                                                                                                                 |      |      | ●    |
| v7               | <b>14.9 <u>Enforce Detail Logging for Access or Changes to Sensitive Data</u></b><br>Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring). |      |      | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1565, T1565.001            | TA0001  | M1022       |

## 6.1.2 Ensure filesystem integrity is regularly checked (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

### Description:

Periodic checking of the filesystem integrity is needed to detect changes to the filesystem.

### Rationale:

Periodic file checking allows the system administrator to determine on a regular basis if critical files have been changed in an unauthorized fashion.

Satisfies: SRG-OS-000363-GPOS-00150, SRG-OS-000446-GPOS-00200, SRG-OS-000447-GPOS-00201

### Audit:

Run the following commands to verify a cron job scheduled to run the aide check.

```
# grep -Ers '^(#[^#]+\s+)?(\/usr\/s?bin\/|^\/s*)aide(\/.wrapper)?\s(--?\S+\s)*(-
-(check|update)|\${AIDEARGS})\b' /etc/cron.* /etc/crontab /var/spool/cron/
```

Ensure a cron job in compliance with site policy is returned.

**- OR -**

Run the following commands to verify that **aidecheck.service** and **aidecheck.timer** are enabled and **aidcheck.timer** is running

```
# systemctl is-enabled aidecheck.service

# systemctl is-enabled aidecheck.timer
# systemctl status aidecheck.timer
```

## Remediation:

- IF - **cron** will be used to schedule and run aide check

Run the following command:

```
# crontab -u root -e
```

Add the following line to the crontab:

```
0 5 * * * /usr/sbin/aide --check
```

- OR -

- IF - **aidecheck.service** and **aidecheck.timer** will be used to schedule and run aide check:

Create or edit the file **/etc/systemd/system/aidecheck.service** and add the following lines:

```
[Unit]
Description=Aide Check

[Service]
Type=simple
ExecStart=/usr/sbin/aide --check

[Install]
WantedBy=multi-user.target
```

Create or edit the file **/etc/systemd/system/aidecheck.timer** and add the following lines:

```
[Unit]
Description=Aide check every day at 5AM

[Timer]
OnCalendar=*-*-* 05:00:00
Unit=aidecheck.service

[Install]
WantedBy=multi-user.target
```

Run the following commands:

```
# chown root:root /etc/systemd/system/aidecheck.*
# chmod 0644 /etc/systemd/system/aidecheck.*

# systemctl daemon-reload

# systemctl enable aidecheck.service
# systemctl --now enable aidecheck.timer
```

## References:

1. <https://github.com/konstruktoid/hardening/blob/master/config/aidecheck.service>
2. <https://github.com/konstruktoid/hardening/blob/master/config/aidecheck.timer>
3. NIST SP 800-53 Rev. 5: AU-2
4. NIST SP 800-53 Revision 5 :: CM-3 (5)

## Additional Information:

The checking in this recommendation occurs every day at 5am. Alter the frequency and time of the checks in compliance with site policy.

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230263  
Rule ID: SV-230263r902716  
STIG ID: RHEL-08-010360  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                  | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.14 Log Sensitive Data Access</b><br>Log sensitive data access, including modification and disposal.                                                                                                                                                                 |      |      | ●    |
| v7               | <b>14.9 Enforce Detail Logging for Access or Changes to Sensitive Data</b><br>Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring). |      |      | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1036, T1036.005            | TA0040  | M1022       |

### *6.1.3 Ensure cryptographic mechanisms are used to protect the integrity of audit tools (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

#### **Rationale:**

Protecting the integrity of the tools used for auditing purposes is a critical step toward ensuring the integrity of audit information. Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Attackers may replace the audit tools or inject code into the existing tools with the purpose of providing the capability to hide or erase system activity from the audit logs.

Audit tools should be cryptographically signed in order to provide the capability to identify when the audit tools have been modified, manipulated, or replaced. An example is a checksum hash of the file or files.

#### **Audit:**

Verify that Advanced Intrusion Detection Environment (AIDE) is properly configured . Run the following script to verify:

- AIDE is configured to use cryptographic mechanisms to protect the integrity of audit tools:
- The following audit tool files include the options "p, i, n, u, g, s, b, acl, xattrs and sha512"
  - auditctl
  - auditd
  - ausearch
  - aureport
  - autrace
  - augenrules

```

#!/usr/bin/env bash

{
    a_output=();a_output2=();a_output3=();a_parlist=()
    l_systemd_analyze="$(whereis systemd-analyze | awk '{print $2}')"
    a_audit_files=("auditctl" "auditd" "ausearch" "aureport" "autrace"
"augenrules")
    f_parameter_chk()
    {
        for l_tool_file in "${a_parlist[@]}"; do
            if grep -Pq -- '\b'"$l_tool_file"' \b' <<< "${!A_out[*]}"; then
                for l_string in "${!A_out[@]}"; do
                    l_check="$(grep -Po --
'^\h*(\usr)?\sbin\/'"$l_tool_file"' \b' <<< "$l_string")"
                    if [ -n "$l_check" ]; then
                        l_fname="$(printf '%s' "${A_out[$l_string]}")"
                        [ "$l_check" != "$(readlink -f "$l_check")" ] && \
                            a_output3+=(" - \"$l_check\" should be updated to:
\"$(readlink -f "$l_check\")\" \" \" in: \"$l_fname\"")
                        a_missing=()
                        for l_var in "${a_items[@]}"; do
                            if ! grep -Pq -- "\b$l_var\b" <<< "$l_string"; then
                                a_missing+=("\"$l_var\"")
                            fi
                        done
                        if [ "${#a_missing[@]}" -gt 0 ]; then
                            a_output2+=(" - Option(s): ( ${a_missing[*]} ) are
missing from: \"$l_tool_file\" in: \"$l_fname\"")
                        else
                            a_output+=(" - Audit tool file \"$l_tool_file\" exists
as: \" \" \"$l_string\" \" \" in the configuration file: \"$l_fname\"")
                        fi
                    fi
                done
            else
                a_output2+=(" - Audit tool file \"$l_tool_file\" doesn't exist in
an AIDE configuration file")
            fi
        done
    }
    f_aide_conf()
    {
        l_config_file="$(whereis aide.conf | awk '{print $2}')"
        if [ -f "$l_config_file" ]; then
            a_items=("p" "i" "n" "u" "g" "s" "b" "acl" "xattrs" "sha512")
            declare -A A_out
            while IFS= read -r l_out; do
                if grep -Pq -- '^ \h* \# \h* \/[^\n\r]+ \.conf \b' <<< "$l_out"; then
                    l_file="${l_out//\# /}"
                else
                    for i in "${a_parlist[@]}"; do
                        grep -Pq -- '^ \h* (\usr)? \sbin\/'"$i"' \b' <<< "$l_out" &&
A_out+=(["$l_out"]="$l_file")
                    done
                fi
            done < < ("$l_systemd_analyze" cat-config "$l_config_file" | grep -
Pio '^ \h* ([^\n\r]+ | \# \h* \/[^\n\r\h]+ \.conf \b) ')

```

```

        if [ "${#A_out[@]}" -gt 0 ]; then
            f_parameter_chk
        else
            a_output2+=(" - No audit tool files are configured in an AIDE
configuration file")
        fi
    else
        a_output2+=(" - AIDE configuration file not found." "    Please
verify AIDE is installed on the system")
    fi
}
for l_audit_file in "${a_audit_files[@]"; do
    if [ -f "$(readlink -f "/sbin/$l_audit_file")" ]; then
        a_parlist+=("$l_audit_file")
    else
        a_output+=(" - Audit tool file \"$(readlink -f
"/sbin/$l_audit_file)\" doesn't exist")
    fi
done
[ "${#a_parlist[@]}" -gt 0 ] && f_aide_conf
if [ "${#a_output2[@]}" -le 0 ]; then
    printf '%s\n' "" "- Audit Result:" "    ** PASS **" "${a_output[@]}"
    [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" "    ** WARNING **"
"${a_output3[@]}"
else
    printf '%s\n' "" "- Audit Result:" "    ** FAIL **" "    * Reasons for
audit failure *" "${a_output2[@]}" ""
    [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' "" "    ** WARNING **"
"${a_output3[@]}"
    [ "${#a_output[@]}" -gt 0 ] && printf '%s\n' "- Correctly set:"
"${a_output[@]}"
fi
}

```

**Note:** The script is written to read the "winning" configuration setting, to include any configuration settings in files included as part of the `@@x_include` setting.



## Remediation:

Run the following command to determine the absolute path to the non-symlinked version on the audit tools:

```
# readlink -f /sbin
```

The output will be either **/usr/sbin** - **OR** - **/sbin**. Ensure the correct path is used. Edit **/etc/aide.conf** and add or update the following selection lines replacing **<PATH>** with the correct path returned in the command above:

```
# Audit Tools
<PATH>/auditctl p+i+n+u+g+s+b+acl+xattrs+sha512
<PATH>/auditd p+i+n+u+g+s+b+acl+xattrs+sha512
<PATH>/ausearch p+i+n+u+g+s+b+acl+xattrs+sha512
<PATH>/aureport p+i+n+u+g+s+b+acl+xattrs+sha512
<PATH>/autrace p+i+n+u+g+s+b+acl+xattrs+sha512
<PATH>/augenrules p+i+n+u+g+s+b+acl+xattrs+sha512
```

### Example

```
# printf '\n%s' "# Audit Tools" "$(readlink -f /sbin/auditctl)
p+i+n+u+g+s+b+acl+xattrs+sha512" "$(readlink -f /sbin/auditd)
p+i+n+u+g+s+b+acl+xattrs+sha512" "$(readlink -f /sbin/ausearch)
p+i+n+u+g+s+b+acl+xattrs+sha512" "$(readlink -f /sbin/aureport)
p+i+n+u+g+s+b+acl+xattrs+sha512" "$(readlink -f /sbin/autrace)
p+i+n+u+g+s+b+acl+xattrs+sha512" "$(readlink -f /sbin/augenrules)
p+i+n+u+g+s+b+acl+xattrs+sha512" >> /etc/aide.conf
```

**Note:** - **IF** - **/etc/aide.conf** includes a **@@x\_include** statement:

*Example:*

```
@@x_include /etc/aide.conf.d ^[a-zA-Z0-9_-]+$
```

- **@@x\_include** FILE
- **@@x\_include** DIRECTORY REGEX
  - **@x\_include** is identical to **@@include**, except that if a config file is executable, it is run and the output is used as config.
  - If the executable file exits with status greater than zero or writes to stderr aide stops with an error.
  - For security reasons DIRECTORY and each executable config file must be owned by the current user and must not be group or world-writable.

## References:

1. AIDE.CONF(5)

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1070, T1070.002, T1083, T1083.000 | TA0007         |                    |

### *6.1.4 Ensure AIDE is configured to use cryptographic mechanisms to protect the integrity of audit tools (Automated)*

**Profile Applicability:**

- STIG

**Description:**

The operating system must use cryptographic mechanisms to protect the integrity of audit tools.

**Rationale:**

Protecting the integrity of the tools used for auditing purposes is a critical step toward ensuring the integrity of audit information. Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

It is not uncommon for attackers to replace the audit tools or inject code into the existing tools with the purpose of providing the capability to hide or erase system activity from the audit logs.

To address this risk, audit tools must be cryptographically signed to provide the capability to identify when the audit tools have been modified, manipulated, or replaced. An example is a checksum hash of the file or files.

## Audit:

Verify that Advanced Intrusion Detection Environment (AIDE) is properly configured to use cryptographic mechanisms to protect the integrity of audit tools.

If AIDE is not installed, ask the System Administrator how file integrity checks are performed on the system.

Check the selection lines to ensure AIDE is configured to add/check with the following command:

```
# grep -E '(\usr\sbin\(audit|au|rsys))' /etc/aide.conf

/usr/sbin/auditctl p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/auditd p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/ausearch p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/aureport p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/autrace p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/rsyslogd p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/auditd p+i+n+u+g+s+b+acl+xattrs+sha512
```

If any of the audit tools listed above do not have an appropriate selection line, ask the system administrator to indicate what cryptographic mechanisms are being used to protect the integrity of the audit tools. If there is no evidence of integrity protection, this is a finding.

## Remediation:

Add or update the following lines to "/etc/aide.conf", to protect the integrity of the audit tools.

```
# Audit Tools
/usr/sbin/auditctl p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/auditd p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/ausearch p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/aureport p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/autrace p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/rsyslogd p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/auditd p+i+n+u+g+s+b+acl+xattrs+sha512
```

## References:

1. NIST SP 800-53 :: AU-9 (3)
2. NIST SP 800-53A :: AU-9 (3).1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230475  
Rule ID: SV-230475r880722  
STIG ID: RHEL-08-030650  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                         | IG 1 | IG 2 | IG 3 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.14 <u>Log Sensitive Data Access</u></b><br>Log sensitive data access, including modification and disposal.                                                                                                                                                                 |      |      | ●    |
| v7               | <b>14.9 <u>Enforce Detail Logging for Access or Changes to Sensitive Data</u></b><br>Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring). |      |      | ●    |

## 6.1.5 Ensure the file integrity tool is configured to verify ACLs (Manual)

### Profile Applicability:

- STIG

### Description:

The operating system's file integrity tool must be configured to verify Access Control Lists (ACLs).

### Rationale:

ACLs can provide permissions beyond those permitted through the file mode and must be verified by file integrity tools.

RHEL 8 installation media come with a file integrity tool, Advanced Intrusion Detection Environment (AIDE).

### Audit:

Verify the file integrity tool is configured to verify ACLs.

Note: AIDE is highly configurable at install time. This requirement assumes the "aide.conf" file is under the "/etc" directory.

If AIDE is not installed, ask the System Administrator how file integrity checks are performed on the system.

Use the following command to determine if the file is in a location other than "/etc/aide/aide.conf":

```
# find / -name aide.conf
```

Check the "aide.conf" file to determine if the "acl" rule has been added to the rule list being applied to the files and directories selection lists with the following command:

```
# grep -E "[+]?acl" /etc/aide.conf
```

```
VarFile = OwnerMode+n+l+X+acl
```

If the "acl" rule is not being used on all selection lines in the "/etc/aide.conf" file, is commented out, or ACLs are not being checked by another file integrity tool, this is a finding.

### Remediation:

Configure the file integrity tool to check file and directory ACLs.

If AIDE is installed, ensure the "acl" rule is present on all file and directory selection lists.

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230552  
Rule ID: SV-230552r880724  
STIG ID: RHEL-08-040310  
Severity: CAT III

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                         | IG 1 | IG 2 | IG 3 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.14 <u>Log Sensitive Data Access</u></b><br>Log sensitive data access, including modification and disposal.                                                                                                                                                                 |      |      | ●    |
| v7               | <b>14.9 <u>Enforce Detail Logging for Access or Changes to Sensitive Data</u></b><br>Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring). |      |      | ●    |

## 6.1.6 Ensure the file integrity tool is configured to verify extended attributes (Manual)

### Profile Applicability:

- STIG

### Description:

The operating system's file integrity tool must be configured to verify extended attributes.

### Rationale:

Extended attributes in file systems are used to contain arbitrary data and file metadata with security implications.

Installation media come with a file integrity tool, Advanced Intrusion Detection Environment (AIDE). Extended attributes in file systems are used to contain arbitrary data and file metadata with security implications.

Installation media come with a file integrity tool, Advanced Intrusion Detection Environment (AIDE).

### Audit:

Verify the file integrity tool is configured to verify extended attributes.

If AIDE is not installed, ask the System Administrator how file integrity checks are performed on the system.

Note: AIDE is highly configurable at install time. This requirement assumes the "aide.conf" file is under the "/etc" directory.

Use the following command to determine if the file is in another location:

```
# find / -name aide.conf
```

Check the "aide.conf" file to determine if the "xattrs" rule has been added to the rule list being applied to the files and directories selection lists.

An example rule that includes the "xattrs" rule follows:

```
All= p+i+n+u+g+s+m+S+sha512+acl+xattrs+selinux
/bin All # apply the custom rule to the files in bin
/sbin All # apply the same custom rule to the files in sbin
```

If the "xattrs" rule is not being used on all uncommented selection lines in the "/etc/aide.conf" file, or extended attributes are not being checked by another file integrity tool, this is a finding.



## Remediation:

Configure the file integrity tool to check file and directory extended attributes.  
If AIDE is installed, ensure the "xattrs" rule is present on all uncommented file and directory selection lists.

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230551  
Rule ID: SV-230551r627750  
STIG ID: RHEL-08-040300  
Severity: CAT III

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                         | IG 1 | IG 2 | IG 3 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>3.14 <u>Log Sensitive Data Access</u></b><br>Log sensitive data access, including modification and disposal.                                                                                                                                                                 |      |      | ●    |
| v7               | <b>14.9 <u>Enforce Detail Logging for Access or Changes to Sensitive Data</u></b><br>Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring). |      |      | ●    |

## 6.2 System Logging

Logging services should be configured to prevent information leaks and to aggregate logs on a remote server so that they can be reviewed in the event of a system compromise. A centralized log server provides a single point of entry for further analysis, monitoring and filtering.

### Security principals for logging

- Ensure transport layer security is implemented between the client and the log server.
- Ensure that logs are rotated as per the environment requirements.
- Ensure all locally generated logs have the appropriate permissions.
- Ensure all security logs are sent to a remote log server.
- Ensure the required events are logged.

### What is covered

This section will cover the minimum best practices for the usage of **either rsyslog or journald**. The recommendations are written such that each is wholly independent of each other and **only one is implemented**.

- If your organization makes use of an enterprise wide logging system completely outside of **rsyslog** or **journald**, then the following recommendations do not directly apply. However, the principals of the recommendations should be followed regardless of what solution is implemented. If the enterprise solution incorporates either of these tools, careful consideration should be given to the following recommendations to determine exactly what applies.
- Should your organization make use of both **rsyslog** and **journald**, take care how the recommendations may or may not apply to you.

### What is not covered

- Enterprise logging systems not utilizing **rsyslog** or **journald**. As logging is very situational and dependent on the local environment, not everything can be covered here.
- Transport layer security should be applied to all remote logging functionality. Both **rsyslog** and **journald** supports secure transport and should be configured as such.
- The log server. There are a multitude of reasons for a centralized log server (and keeping a short period of logging on the local system), but the log server is out of scope for these recommendations.

## 6.2.1 Configure journald

Included in the systemd suite is a journaling service called **systemd-journald.service** for the collection and storage of logging data. It creates and maintains structured, indexed journals based on logging information that is received from a variety of sources such as:

- Classic RFC3164 BSD syslog via the /dev/log socket
- STDOUT/STDERR of programs via StandardOutput=journal + StandardError=journal in service files (both of which are default settings)
- Kernel log messages via the /dev/kmsg device node
- Audit records via the kernel's audit subsystem
- Structured log messages via journald's native protocol

Any changes made to the **systemd-journald** configuration will require a re-start of **systemd-journald**

### 6.2.1.1 Configure systemd-journald service

**systemd-journald** is a system service that collects and stores logging data. It creates and maintains structured, indexed journals based on logging information that is received from a variety of sources:

- Kernel log messages, via kmsg
- Simple system log messages, via the libc syslog call
- Structured system log messages via the native Journal API
- Standard output and standard error of service units
- Audit records, originating from the kernel audit subsystem

The daemon will implicitly collect numerous metadata fields for each log messages in a secure and unfakeable way. See `systemd.journal-fields` man page for more information about the collected metadata.

The journal service stores log data either persistently below `/var/log/journal` or in a volatile way below `/run/log/journal/`. By default, log data is stored persistently if `/var/log/journal/` exists during boot, with an implicit fallback to volatile storage. Use **Storage=** in `journald.conf` to configure where log data is placed, independently of the existence of `/var/log/journal/`.

On systems where `/var/log/journal/` does not exist but where persistent logging is desired, and the default `journald.conf` is used, it is sufficient to create the directory and ensure it has the correct access modes and ownership.

### 6.2.1.1.1 Ensure journald service is enabled and active (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

Ensure that the **systemd-journald** service is enabled to allow capturing of logging events.

#### Rationale:

If the **systemd-journald** service is not enabled to start on boot, the system will not capture logging events.

#### Audit:

Run the following command to verify **systemd-journald** is enabled:

```
# systemctl is-enabled systemd-journald.service  
  
static
```

**Note:** By default the **systemd-journald** service does not have an **[Install]** section and thus cannot be enabled / disabled. It is meant to be referenced as **Requires** or **Wants** by other unit files. As such, if the status of **systemd-journald** is not **static**, investigate why

Run the following command to verify **systemd-journald** is active:

```
# systemctl is-active systemd-journald.service  
  
active
```

#### Remediation:

Run the following commands to unmask and start **systemd-journald.service**

```
# systemctl unmask systemd-journald.service  
# systemctl start systemd-journald.service
```

#### References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-7 AU-12

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                         |  |  |  |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          |  |  |  |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. |                                                                                     |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1562, T1562.001 | TA0005  | M1029       |

## 6.2.1.1.2 Ensure journald log file access is configured (Manual)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Journald will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

### Rationale:

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

### Audit:

First determine if there is an override file `/etc/tmpfiles.d/systemd.conf`. If so, this file will override all default settings as defined in `/usr/lib/tmpfiles.d/systemd.conf` and should be inspected.

If no override file exists, inspect the default `/usr/lib/tmpfiles.d/systemd.conf` against the site specific requirements.

Ensure that file permissions are mode `0640` or more restrictive.

Run the following script to verify if an override file exists or not and if the files permissions are mode `640` or more restrictive:

```
#!/usr/bin/env bash

{
    l_output="" file_path=""
    # Check for the existence of an override file
    if [ -f /etc/tmpfiles.d/systemd.conf ]; then
        file_path="/etc/tmpfiles.d/systemd.conf"
    elif [ -f /usr/lib/tmpfiles.d/systemd.conf ]; then
        file_path="/usr/lib/tmpfiles.d/systemd.conf"
    fi
    if [ -n "$file_path" ]; then # Ensure a file path is found
        higher_permissions_found=false # Initialize a flag to check if
higher permissions are found
        # Read the file line by line and check for permissions higher than
0640
        while IFS= read -r line; do
            if echo "$line" | grep -Piq '\s*[a-z]+\s+[\^s]+\s+0*([6-7][4-
7][1-7]|7[0-7][0-7])\s+'; then
                higher_permissions_found=true
                break
            fi
        done < "$file_path"
        if $higher_permissions_found; then
            echo -e "\n - permissions other than 0640 found in $file_path"
            l_output="$l_output\n - Inspect $file_path"
        else
            echo -e "All permissions inside $file_path are 0640 or more
restrictive."
        fi
    fi
    if [ -z "$l_output" ]; then # Provide output from checks
        echo -e "\n- Audit Result:\n  ** PASS **\n$line exists and has
correct permissions set\n"
    else
        echo -e "\n- Audit Result:\n  ** REVIEW **\n$l_output\n - Review
permissions to ensure they are set IAW site policy"
    fi
}

```

## Remediation:

If the default configuration is not appropriate for the site specific requirements, copy [/usr/lib/tmpfiles.d/systemd.conf](#) to [/etc/tmpfiles.d/systemd.conf](#) and modify as required. Requirements is either **0640** or site policy if that is less restrictive.

## References:

1. NIST SP 800-53 Rev. 5: AC-3, AU-2, AU-12, MP-2, SI-5

## Additional Information:

See [man 5 tmpfiles.d](#) for detailed information on the permission sets for the relevant log files. Further information with examples can be found at <https://www.freedesktop.org/software/systemd/man/tmpfiles.d.html>



### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1083, T1083.000 | TA0007  | M1022       |

### 6.2.1.1.3 Ensure journald log file rotation is configured (Manual)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

Journald includes the capability of rotating log files regularly to avoid filling up the system with logs or making the logs unmanageably large. The file `/etc/systemd/journald.conf` is the configuration file used to specify how logs generated by Journald should be rotated.

#### Rationale:

By keeping the log files smaller and more manageable, a system administrator can easily archive these files to another system and spend less time looking through inordinately large log files.

#### Audit:

Review `/etc/systemd/journald.conf` and files in the `/etc/systemd/journald.conf.d/` directory ending in `.conf`. Verify logs are rotated according to site policy. The specific parameters for log rotation are:

```
SystemMaxUse=  
SystemKeepFree=  
RuntimeMaxUse=  
RuntimeKeepFree=  
MaxFileSec=
```

#### Remediation:

Edit `/etc/systemd/journald.conf` or a file ending in `.conf` the `/etc/systemd/journald.conf.d/` directory. Set the following parameters in the `[Journal]` section to ensure logs are rotated according to site policy. The settings should be carefully understood as there are specific edge cases and prioritization of parameters.

The specific parameters for log rotation are:

```
SystemMaxUse=  
SystemKeepFree=  
RuntimeMaxUse=  
RuntimeKeepFree=  
MaxFileSec=
```

**Note:** If these settings appear in a canonically later file, or later in the same file, the setting will be overwritten

## References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-7, AU-12

## Additional Information:

See [man 5 journald.conf](#) for detailed information regarding the parameters in use.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                         |  |  |  |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          |  |  |  |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. |                                                                                     |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1070, T1070.002            | TA0040  | M1022       |

#### 6.2.1.1.4 Ensure journald ForwardToSyslog is disabled (Automated)

##### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

##### Description:

Data from **journald** should be kept in the confines of the service and not forwarded to other services.

##### Rationale:

- IF - **journald** is the method for capturing logs, all logs of the system should be handled by **journald** and not forwarded to other logging mechanisms.

**Note:** This recommendation **only applies if journald is the chosen method for client side logging**. Do not apply this recommendation if **rsyslog** is used.

##### Audit:

- IF - **journald** is the method for capturing logs  
Run the following script to verify **ForwardToSyslog** is not set to **yes**:

```
#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_parlist=("ForwardToSyslog=yes")
    l_systemd_config_file="/etc/systemd/journald.conf" # Main systemd configuration
file
    config_file_parameter_chk()
    {
        unset A_out; declare -A A_out # Check config file(s) setting
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//\# /}"
                else
                    l_systemd_parameter="$(awk -F= '{print $1}' <<< "$l_out" | xargs) "
                    grep -Piq -- "\^h*$l_systemd_parameter_name\b" <<<
"$l_systemd_parameter" && A_out+=(["$l_systemd_parameter"]="$l_file")
                fi
            fi
        done < <(/usr/bin/systemd-analyze cat-config "$l_systemd_config_file" | grep -
Pio '\^h*([\^#\n\r]+|#[\^#\n\r\h]+\.\conf\b)')
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS="" read -r l_systemd_file_parameter_name
l_systemd_file_parameter_value; do
                l_systemd_file_parameter_name="${l_systemd_file_parameter_name// /}"
                l_systemd_file_parameter_value="${l_systemd_file_parameter_value// /}"
                if ! grep -Piq "\^h*$l_systemd_parameter_value\b" <<<
"$l_systemd_file_parameter_value"; then
                    l_output="$l_output\n - \"$l_systemd_parameter_name\" is correctly set
to \"$l_systemd_file_parameter_value\" in \"$(printf '%s' "${A_out[@]}")\""\n"
                else
                    l_output2="$l_output2\n - \"$l_systemd_parameter_name\" is incorrectly
set to \"$l_systemd_file_parameter_value\" in \"$(printf '%s' "${A_out[@]}")\""\n"
                fi
            done < <(grep -Pio -- "\^h*$l_systemd_parameter_name\h*=\h*\H+"
"$${A_out[@]}")
        else
            l_output="$l_output\n - \"$l_systemd_parameter_name\" is not set in an
included file\n    ** Note: \"$l_systemd_parameter_name\" May be set in a file that's
ignored by load procedure **\n"
        fi
    }
    while IFS="" read -r l_systemd_parameter_name l_systemd_parameter_value; do #
Assess and check parameters
        l_systemd_parameter_name="${l_systemd_parameter_name// /}"
        l_systemd_parameter_value="${l_systemd_parameter_value// /}"
        config_file_parameter_chk
        done < <(printf '%s\n' "${a_parlist[@]}")
        if [ -z "$l_output2" ]; then # Provide output from checks
            echo -e "\n- Audit Result:\n    ** PASS **\n$l_output\n"
        else
            echo -e "\n- Audit Result:\n    ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2\n"
            [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
        fi
    }
}
```

## Remediation:

- IF - **rsyslog** is the preferred method for capturing logs, this section and Recommendation should be skipped and the "Configure rsyslog" section followed.
- IF - **journald** is the preferred method for capturing logs:  
Set the following parameter in the **[Journal]** section in **/etc/systemd/journald.conf** or a file in **/etc/systemd/journald.conf.d/** ending in **.conf**:

```
ForwardToSyslog=no
```

### Example:

```
#!/usr/bin/env bash

{
    [ ! -d /etc/systemd/journald.conf.d/ ] && mkdir
    /etc/systemd/journald.conf.d/
    if grep -Psq -- '^\h*\[Journal\] /etc/systemd/journald.conf.d/60-
journald.conf; then
        printf '%s\n' "ForwardToSyslog=no" >> /etc/systemd/journald.conf.d/60-
journald.conf
    else
        printf '%s\n' "[Journal]" "ForwardToSyslog=no" >>
/etc/systemd/journald.conf.d/60-journald.conf
    fi
}
```

**Note:** If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten

Run to following command to update the parameters in the service:

```
# systemctl reload-or-restart systemd-journald
```

## Default Value:

ForwardToSyslog=no

## References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-6, AU-7, AU-12

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                         |  |  |  |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. |                                                                                     |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1562, T1562.006 | TA0040  | M1029       |

### *6.2.1.1.5 Ensure journald Storage is configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Data from journald may be stored in volatile memory or persisted locally on the server. Logs in memory will be lost upon a system reboot. By persisting logs to local disk on the server they are protected from loss due to a reboot.

#### **Rationale:**

Writing log data to disk will provide the ability to forensically reconstruct events which may have impacted the operations or security of a system even after a system crash or reboot.

#### **Audit:**

Run the following script to verify **Storage** is set to **persistent**:



```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_parlist=("Storage=persistent")
    l_systemd_config_file="/etc/systemd/journald.conf" # Main systemd configuration
file
    config_file_parameter_chk()
    {
        unset A_out; declare -A A_out # Check config file(s) setting
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//\# /}"
                else
                    l_systemd_parameter="$(awk -F= '{print $1}' <<< "$l_out" | xargs) "
                    grep -Piq -- "\^h*$l_systemd_parameter_name\b" <<<
"$l_systemd_parameter" && A_out+=(["$l_systemd_parameter"]="$l_file")
                fi
            fi
        done < <(/usr/bin/systemd-analyze cat-config "$l_systemd_config_file" | grep -
Pio '\^h*([\^#\n\r]+|#[\h*\n\r\h]+\.\conf\b)')
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS="" read -r l_systemd_file_parameter_name
l_systemd_file_parameter_value; do
                l_systemd_file_parameter_name="${l_systemd_file_parameter_name// /}"
                l_systemd_file_parameter_value="${l_systemd_file_parameter_value// /}"
                if grep -Piq "\^h*$l_systemd_parameter_value\b" <<<
"$l_systemd_file_parameter_value"; then
                    l_output="$l_output\n - \"$l_systemd_parameter_name\" is correctly set
to \"$l_systemd_file_parameter_value\" in \"$(printf '%s' "${A_out[@]}")\""\n"
                else
                    l_output2="$l_output2\n - \"$l_systemd_parameter_name\" is incorrectly
set to \"$l_systemd_file_parameter_value\" in \"$(printf '%s' "${A_out[@]}")\" and
should have a value matching: \"$l_systemd_parameter_value\""\n"
                fi
            done < <(grep -Pio -- "\^h*$l_systemd_parameter_name\h*=\h*\H+"
"$${A_out[@]}")
        else
            l_output2="$l_output2\n - \"$l_systemd_parameter_name\" is not set in an
included file\n  ** Note: \"$l_systemd_parameter_name\" May be set in a file that's
ignored by load procedure **"\n"
        fi
    }
    while IFS="" read -r l_systemd_parameter_name l_systemd_parameter_value; do #
Assess and check parameters
        l_systemd_parameter_name="${l_systemd_parameter_name// /}"
        l_systemd_parameter_value="${l_systemd_parameter_value// /}"
        config_file_parameter_chk
        done < <(printf '%s\n' "${a_parlist[@]}")
        if [ -z "$l_output2" ]; then # Provide output from checks
            echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
        else
            echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2"
            [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
        fi
    fi
}

```

## Remediation:

Set the following parameter in the **[Journal]** section in **/etc/systemd/journald.conf** or a file in **/etc/systemd/journald.conf.d/** ending in **.conf**:

```
Storage=persistent
```

### Example:

```
#!/usr/bin/env bash

{
    [ ! -d /etc/systemd/journald.conf.d/ ] && mkdir
    /etc/systemd/journald.conf.d/
    if grep -Psq -- '^h*\[Journal\]' /etc/systemd/journald.conf.d/60-
journald.conf; then
        printf '%s\n' "Storage=persistent" >> /etc/systemd/journald.conf.d/60-
journald.conf
    else
        printf '%s\n' "[Journal]" "Storage=persistent" >>
/etc/systemd/journald.conf.d/60-journald.conf
    fi
}
```

**Note:** If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten

Run to following command to update the parameters in the service:

```
# systemctl reload-or-restart systemd-journald
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3, AU-12

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                         | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.2 Collect Audit Logs</b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                         |  |  |  |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          |  |  |  |
| v7               | <b>6.3 Enable Detailed Logging</b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. |                                                                                       |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1562, T1562.006 | TA0005  | M1022       |

### *6.2.1.1.6 Ensure journald Compress is configured (Automated)*

**Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

**Description:**

The journald system includes the capability of compressing overly large files to avoid filling up the system with logs or making the logs unmanageably large.

**Rationale:**

Uncompressed large files may unexpectedly fill a filesystem leading to resource unavailability. Compressing logs prior to write can prevent sudden, unexpected filesystem impacts.

**Audit:**

Run the following script to verify **Compress** is set to **yes**:

```

#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_parlist=("Compress=yes")
    l_systemd_config_file="/etc/systemd/journald.conf" # Main systemd configuration
file
    config_file_parameter_chk()
    {
        unset A_out; declare -A A_out # Check config file(s) setting
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="${l_out//\# /}"
                else
                    l_systemd_parameter="$(awk -F= '{print $1}' <<< "$l_out" | xargs) "
                    grep -Piq -- "\^h*$l_systemd_parameter_name\b" <<<
"$l_systemd_parameter" && A_out+=(["$l_systemd_parameter"]="$l_file")
                fi
            fi
        done < <(/usr/bin/systemd-analyze cat-config "$l_systemd_config_file" | grep -
Pio '\^h*([\^#\n\r]+|#[\h*\n\r\h]+\.\conf\b)')
        if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
            while IFS="" read -r l_systemd_file_parameter_name
l_systemd_file_parameter_value; do
                l_systemd_file_parameter_name="${l_systemd_file_parameter_name// /}"
                l_systemd_file_parameter_value="${l_systemd_file_parameter_value// /}"
                if grep -Piq "\^h*$l_systemd_parameter_value\b" <<<
"$l_systemd_file_parameter_value"; then
                    l_output="$l_output\n - \"$l_systemd_parameter_name\" is correctly set
to \"$l_systemd_file_parameter_value\" in \"$(printf '%s' "${A_out[@]}")\""\n"
                else
                    l_output2="$l_output2\n - \"$l_systemd_parameter_name\" is incorrectly
set to \"$l_systemd_file_parameter_value\" in \"$(printf '%s' "${A_out[@]}")\" and
should have a value matching: \"$l_systemd_parameter_value\""\n"
                fi
            done < <(grep -Pio -- "\^h*$l_systemd_parameter_name\h*=\h*\H+"
"$${A_out[@]}")
        else
            l_output2="$l_output2\n - \"$l_systemd_parameter_name\" is not set in an
included file\n  ** Note: \"$l_systemd_parameter_name\" May be set in a file that's
ignored by load procedure **"\n"
        fi
    }
    while IFS="" read -r l_systemd_parameter_name l_systemd_parameter_value; do #
Assess and check parameters
        l_systemd_parameter_name="${l_systemd_parameter_name// /}"
        l_systemd_parameter_value="${l_systemd_parameter_value// /}"
        config_file_parameter_chk
        done < <(printf '%s\n' "${a_parlist[@]}")
        if [ -z "$l_output2" ]; then # Provide output from checks
            echo -e "\n- Audit Result:\n  ** PASS **\n$l_output\n"
        else
            echo -e "\n- Audit Result:\n  ** FAIL **\n - Reason(s) for audit
failure:\n$l_output2"
            [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
        fi
    fi
}

```

## Remediation:

Set the following parameter in the **[Journal]** section in **/etc/systemd/journald.conf** or a file in **/etc/systemd/journald.conf.d/** ending in **.conf**:

```
Compress=yes
```

### Example:

```
#!/usr/bin/env bash

{
    [ ! -d /etc/systemd/journald.conf.d/ ] && mkdir
    /etc/systemd/journald.conf.d/
    if grep -Psq -- '^\\h*\\[Journal\\]' /etc/systemd/journald.conf.d/60-
journald.conf; then
        printf '%s\\n' "Compress=yes" >> /etc/systemd/journald.conf.d/60-
journald.conf
    else
        printf '%s\\n' "[Journal]" "Compress=yes" >>
/etc/systemd/journald.conf.d/60-journald.conf
    fi
}
```

**Note:** If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten

Run the following command to update the parameters in the service:

```
# systemctl reload-or-restart systemd-journald
```

## References:

1. NIST SP 800-53 Rev. 5: AU-4

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                         | ●    | ●    | ●    |
| v8               | <b>8.3 <u>Ensure Adequate Audit Log Storage</u></b><br>Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.                                        | ●    | ●    | ●    |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          | ●    | ●    | ●    |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. |      | ●    | ●    |
| v7               | <b>6.4 <u>Ensure adequate storage for logs</u></b><br>Ensure that all systems that store logs have adequate storage space for the logs generated.                                                                      |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.001            | TA0040  | M1053       |

### 6.2.1.2 Configure systemd-journal-remote

The `systemd-journal-remote` package includes `systemd-journal-upload`.

`systemd-journal-upload` will upload journal entries to the URL specified with `--url=`. This program reads journal entries from one or more journal files, similarly to `journalctl`.

`systemd-journal-upload` transfers the raw content of journal file and uses HTTP as a transport protocol.

`systemd-journal-upload.service` is a system service that uses `systemd-journal-upload` to upload journal entries to a server. It uses the configuration in `journal-upload.conf`.



### 6.2.1.2.1 Ensure systemd-journal-remote is installed (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

Journald **systemd-journal-remote** supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralized log management.

#### Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

#### Audit:

- IF - **journal**d will be used for logging on the system:

Run the following command to verify **systemd-journal-remote** is installed.

```
# rpm -q systemd-journal-remote
```

Verify the output matches:

```
systemd-journal-remote-<version>
```

#### Remediation:

Run the following command to install **systemd-journal-remote**:

```
# dnf install systemd-journal-remote
```

#### References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-7 AU-12

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                         |  |  |  |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          |  |  |  |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. |                                                                                     |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1562, T1562.006 | TA0040  | M1029       |

## 6.2.1.2.2 Ensure systemd-journal-remote authentication is configured (Manual)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Journald **systemd-journal-upload** supports the ability to send log events it gathers to a remote log host.

### Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

### Audit:

Run the following command to verify **systemd-journal-upload** authentication is configured:

```
# grep -P "^ *URL=|^ *ServerKeyFile=|^ *ServerCertificateFile=|^ *TrustedCertificateFile=" /etc/systemd/journal-upload.conf
```

Verify the output matches per your environments certificate locations and the URL of the log server:

*Example:*

```
[Upload]
URL=192.168.50.42
ServerKeyFile=/etc/ssl/private/journal-upload.pem
ServerCertificateFile=/etc/ssl/certs/journal-upload.pem
TrustedCertificateFile=/etc/ssl/ca/trusted.pem
```

## Remediation:

Edit the `/etc/systemd/journal-upload.conf` file or a file in `/etc/systemd/journal-upload.conf.d` ending in `.conf` and ensure the following lines are set in the `[Upload]` section per your environment:

```
[Upload]
URL=192.168.50.42
ServerKeyFile=/etc/ssl/private/journal-upload.pem
ServerCertificateFile=/etc/ssl/certs/journal-upload.pem
TrustedCertificateFile=/etc/ssl/ca/trusted.pem
```

Restart the service:

```
# systemctl restart systemd-journal-upload
```

## References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-12

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                         | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.2 Collect Audit Logs</b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                         |  |  |  |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          |  |  |  |
| v7               | <b>6.3 Enable Detailed Logging</b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. |                                                                                       |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1562, T1562.006 | TA0040  | M1029       |

### 6.2.1.2.3 Ensure systemd-journal-upload is enabled and active (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

Journald **systemd-journal-upload** supports the ability to send log events it gathers to a remote log host.

#### Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

#### Audit:

Run the following command to verify **systemd-journal-upload** is enabled.

```
# systemctl is-enabled systemd-journal-upload.service
enabled
```

Run the following command to verify **systemd-journal-upload** is active:

```
# systemctl is-active systemd-journal-upload.service
active
```

#### Remediation:

Run the following commands to unmask, enable and start **systemd-journal-upload**:

```
# systemctl unmask systemd-journal-upload.service
# systemctl --now enable systemd-journal-upload.service
```

#### References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-12

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                         |  |  |  |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          |  |  |  |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. |                                                                                     |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1562, T1562.006 | TA0040  | M1029       |

#### 6.2.1.2.4 Ensure systemd-journal-remote service is not in use (Automated)

##### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

##### Description:

Journald **systemd-journal-remote** supports the ability to receive messages from remote hosts, thus acting as a log server. Clients should not receive data from other hosts.

##### NOTE:

- The same package, **systemd-journal-remote**, is used for both sending logs to remote hosts and receiving incoming logs.
- With regards to receiving logs, there are two services; **systemd-journal-remote.socket** and **systemd-journal-remote.service**.

##### Rationale:

If a client is configured to also receive data, thus turning it into a server, the client system is acting outside it's operational boundary.

##### Audit:

Run the following command to verify **systemd-journal-remote.socket** and **systemd-journal-remote.service** are not enabled:

```
# systemctl is-enabled systemd-journal-remote.socket systemd-journal-remote.service | grep -P -- '^enabled'
```

Nothing should be returned

Run the following command to verify **systemd-journal-remote.socket** and **systemd-journal-remote.service** are not active:

```
# systemctl is-active systemd-journal-remote.socket systemd-journal-remote.service | grep -P -- '^active'
```

Nothing should be returned

## Remediation:

Run the following commands to stop and mask **systemd-journal-remote.socket** and **systemd-journal-remote.service**:

```
# systemctl stop systemd-journal-remote.socket systemd-journal-remote.service
# systemctl mask systemd-journal-remote.socket systemd-journal-remote.service
```

## References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-7 AU-12

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      | ●    | ●    |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      | ●    | ●    |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1562, T1562.006 | TA0040  | M1029       |



## 6.2.2 Configure rsyslog

The **rsyslog** software package may be used instead of the default **journald** logging mechanism.

Rsyslog has evolved over several decades. For this reason it supports three different configuration formats (“languages”):

- **basic** - previously known as the **sysklogd** format, this is the format best used to express basic things, such as where the statement fits on a single line.
  - It stems back to the original syslog.conf format, in use now for several decades.
  - The most common use case is matching on facility/severity and writing matching messages to a log file.
- **advanced** - previously known as the **RainerScript** format, this format was first available in rsyslog v6 and is the current, best and most precise format for non-trivial use cases where more than one line is needed.
  - Prior to v7, there was a performance impact when using this format that encouraged use of the basic format for best results. Current versions of rsyslog do not suffer from this (historical) performance impact.
  - This new style format is specifically targeted towards more advanced use cases like forwarding to remote hosts that might be partially offline.
- **obsolete legacy** - previously known simply as the **legacy** format, this format is exactly what its name implies: it is obsolete and should not be used when writing new configurations. It was created in the early days (up to rsyslog version 5) where we expected that rsyslog would extend sysklogd just mildly. Consequently, it was primarily aimed at small additions to the original sysklogd format.
  - Practice has shown that it was notoriously hard to use for more advanced use cases, and thus we replaced it with the advanced format.
  - In essence, everything that needs to be written on a single line that starts with a dollar sign is legacy format. Users of this format are encouraged to migrate to the basic or advanced formats.

**Note:** This section only applies if **rsyslog** is the chosen method for client side logging. Do not apply this section if **journald** is used.

### 6.2.2.1 Ensure rsyslog is installed (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

#### Description:

The **rsyslog** software is recommended in environments where **journald** does not meet operation requirements.

#### Rationale:

The security enhancements of **rsyslog** such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server) justify installing and configuring the package.

#### Audit:

- **IF** - **rsyslog** is being used for logging on the system:  
Run the following command to verify **rsyslog** is installed:

```
# rpm -q rsyslog
```

Verify the output matches:

```
rsyslog-<version>
```

#### Remediation:

Run the following command to install **rsyslog**:

```
# dnf install rsyslog
```

#### Default Value:

Installed

#### References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230477  
RULE ID: SV-230477r627750  
STIG ID: RHEL-08-030670  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                         | IG 1                                                                                | IG 2                                                                                 | IG 3                                                                                 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| v8               | <b>8.2 Collect Audit Logs</b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                         |  |   |   |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          |  |   |   |
| v7               | <b>6.3 Enable Detailed Logging</b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. |                                                                                     |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations  |
|------------------------------------|---------|--------------|
| T1005, T1005.000, T1070, T1070.002 | TA0005  | M1029, M1057 |

## 6.2.2.2 Ensure rsyslog service is enabled and active (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Once the **rsyslog** package is installed, ensure that the service is enabled.

### Rationale:

If the **rsyslog** service is not enabled to start on boot, the system will not capture logging events.

### Audit:

- **IF** - **rsyslog** is being used for logging on the system:  
Run the following command to verify **rsyslog.service** is enabled:

```
# systemctl is-enabled rsyslog  
  
enabled
```

Run the following command to verify **rsyslog.service** is active:

```
# systemctl is-active rsyslog.service  
  
active
```

### Remediation:

- **IF** - **rsyslog** is being used for logging on the system:  
Run the following commands to unmask, enable, and start **rsyslog.service**:

```
# systemctl unmask rsyslog.service  
# systemctl enable rsyslog.service  
# systemctl start rsyslog.service
```

### References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-3, AU-12

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                         |  |  |  |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          |  |  |  |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. |                                                                                     |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques               | Tactics | Mitigations |
|-------------------------------------------|---------|-------------|
| T1070, T1070.002, T1211, T1562, T1562.001 | TA0005  | M1029       |

### *6.2.2.3 Ensure all remote access methods are monitored (Automated)*

**Profile Applicability:**

- STIG

**Description:**

Remote access is access to a system by an authorized user communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

**Rationale:**

Remote access services, such as those providing remote access to network devices and information systems, which lack automated monitoring capabilities, increase risk and make remote user access management difficult at best.

Automated monitoring of remote access sessions allows organizations to detect cyber attacks and ensure ongoing compliance with remote access policies by auditing connection activities of remote access capabilities, such as Remote Desktop Protocol (RDP), on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

**Audit:**

Run the following script to verify remote access methods are being logged by sending **auth**, **authpriv**, and **daemon** events to **/var/log/secure**:



## Remediation:

Run the following command to install **rsyslog**:

```
# ! rpm -q rsyslog &>/dev/null && dnf install rsyslog
```

Add or update the following lines to the **/etc/rsyslog.conf** file:

```
auth.*;authpriv.*;daemon.* /var/log/secure
```

Run the following command to load the changes to **rsyslog.service**

```
# systemctl reload-or-restart rsyslog.service
```

## References:

1. NIST SP 800-53 :: AC-17 (1)
2. NIST SP 800-53A :: AC-17 (1).1

## Additional Information:

Red Hat Enterprise Linux 8

```
Red Hat Enterprise Linux 8
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230228
RULE ID: SV-230228r951592
STIG ID: RHEL-08-010070
SEVERITY: CAT II
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                         |  |  |  |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. |                                                                                       |  |  |



**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1070, T1070.002                   | TA0005         | M1047              |

## 6.2.2.4 Ensure journald is configured to send logs to rsyslog (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Data from **systemd-journald** may be stored in volatile memory or persisted locally on the server. Utilities exist to accept remote export of **systemd-journald** logs, however, use of the **rsyslog** service provides a consistent means of log collection and export.

### Rationale:

- **IF** - **rsyslog** is the preferred method for capturing logs, all logs of the system should be sent to it for further processing.

**Note:** This recommendation **only applies if rsyslog is the chosen method for client side logging**. Do not apply this recommendation if **systemd-journald** is used.

### Audit:

- **IF** - **rsyslog** is the preferred method for capturing logs  
Run the following script to verify that logs are forwarded to **rsyslog** by setting **ForwardToSyslog** to **yes** in the **systemd-journald** configuration:

```
#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_parlist=("ForwardToSyslog=yes")
    l_systemd_config_file="/etc/systemd/journald.conf" # Main systemd configuration file
    config_file_parameter_chk()
    {
        unset A_out; declare -A A_out # Check config file(s) setting
        while read -r l_out; do
            if [ -n "$l_out" ]; then
                if [[ $l_out =~ ^\s*# ]]; then
                    l_file="$l_out// # //"
                else
                    l_systemd_parameter="$(awk -F= '{print $1}' <<< "$l_out" | xargs)"
                    grep -Piq -- "\h*$l_systemd_parameter_name\b" <<< "$l_systemd_parameter" &&
                    A_out+=(["$l_systemd_parameter"]="$l_file")
                fi
            fi
            done < <(/usr/bin/systemd-analyze cat-config "$l_systemd_config_file" | grep -Pio
            '\h*([\h*\n\r]+|\h*\[/[\h*\n\r\h]+\.\conf\b)')
            if (( ${#A_out[@]} > 0 )); then # Assess output from files and generate output
                while IFS="" read -r l_systemd_file_parameter_name l_systemd_file_parameter_value; do
                    l_systemd_file_parameter_name="$l_systemd_file_parameter_name// //"
                    l_systemd_file_parameter_value="$l_systemd_file_parameter_value// //"
                    if grep -Piq "\h*$l_systemd_file_parameter_name\b" <<<
                    "$l_systemd_file_parameter_value"; then
                        l_output="$l_output\n - \"$l_systemd_file_parameter_name\" is correctly set to
                        \"$l_systemd_file_parameter_value\" in \"$(printf '%s' "${A_out[@]}")\""\n"
                    else
                        l_output2="$l_output2\n - \"$l_systemd_file_parameter_name\" is incorrectly set to
                        \"$l_systemd_file_parameter_value\" in \"$(printf '%s' "${A_out[@]}")\" and should have a value
                        matching: \"$l_systemd_file_parameter_value\""\n"
                    fi
                done < <(grep -Pio -- "\h*$l_systemd_file_parameter_name\b" <<< "${A_out[@]}")
            else
                l_output2="$l_output2\n - \"$l_systemd_file_parameter_name\" is not set in an included file\n
                ** Note: \"$l_systemd_file_parameter_name\" May be set in a file that's ignored by load procedure
                **\n"
            fi
        }
        while IFS="" read -r l_systemd_parameter_name l_systemd_parameter_value; do # Assess and
        check parameters
            l_systemd_parameter_name="$l_systemd_parameter_name// //"
            l_systemd_parameter_value="$l_systemd_parameter_value// //"
            config_file_parameter_chk
            done < <(printf '%s\n' "${a_parlist[@]}")
            if [ -z "$l_output2" ]; then # Provide output from checks
                echo -e "\n- Audit Result:\n ** PASS **\n$l_output\n"
            else
                echo -e "\n- Audit Result:\n ** FAIL **\n - Reason(s) for audit failure:\n$l_output2"
                [ -n "$l_output" ] && echo -e "\n- Correctly set:\n$l_output\n"
            fi
        }
    }
}
```

Run the following command to verify **systemd-journald.service** and **rsyslog.service** are loaded and active:

```
# systemctl list-units --type service | grep -P -- '(journald|rsyslog)'
```

Output should be similar to:

|                          |                       |
|--------------------------|-----------------------|
| rsyslog.service          | loaded active running |
| System Logging Service   |                       |
| systemd-journald.service | loaded active running |
| Journal Service          |                       |

## Remediation:

- **IF - Journald** is the preferred method for capturing logs, this section and Recommendation should be skipped and the "Configure Journald" section followed.

- **IF - rsyslog** is the preferred method for capturing logs:

Set the following parameter in the **[Journal]** section in **/etc/systemd/journald.conf** or a file in **/etc/systemd/journald.conf.d/** ending in **.conf**:

```
ForwardToSyslog=yes
```

### Example:

```
#!/usr/bin/env bash

{
    [ ! -d /etc/systemd/journald.conf.d/ ] && mkdir
    /etc/systemd/journald.conf.d/
    if grep -Psq -- '^\h*\[Journal\] /etc/systemd/journald.conf.d/60-
journald.conf; then
        printf '%s\n' "ForwardToSyslog=yes" >> /etc/systemd/journald.conf.d/60-
journald.conf
    else
        printf '%s\n' "[Journal]" "ForwardToSyslog=yes" >>
/etc/systemd/journald.conf.d/60-journald.conf
    fi
}
```

**Note:** If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten

Run to following command to update the parameters in the service:

Restart **systemd-journald.service**:

```
# systemctl reload-or-restart systemd-journald.service
```

## References:

1. NIST SP 800-53 Rev. 5: AC-3, AU-2, AU-4, AU-12, MP-2
2. SYSTEMD-JOURNALD.SERVICE(8)
3. JOURNALD.CONF(5)

## Additional Information:

As noted in the `systemd-journald` man pages, `systemd-journald` logs may be exported to `rsyslog` either through the process mentioned here, or through a facility like `systemd-journald.service`. There are trade-offs involved in each implementation, where `ForwardToSyslog` will immediately capture all events (and forward to an external log server, if properly configured), but may not capture all boot-up activities. Mechanisms such as `systemd-journald.service`, on the other hand, will record bootup events, but may delay sending the information to `rsyslog`, leading to the potential for log manipulation prior to export. Be aware of the limitations of all tools employed to secure a system.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                         |    |    |    |
| v8               | <b>8.9 <u>Centralize Audit Logs</u></b><br>Centralize, to the extent possible, audit log collection and retention across enterprise assets.                                                                            |                                                                                       |    |    |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          |  |  |  |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. |                                                                                       |  |  |
| v7               | <b>6.5 <u>Central Log Management</u></b><br>Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.                                                              |                                                                                       |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques               | Tactics | Mitigations |
|-------------------------------------------|---------|-------------|
| T1070, T1070.002, T1562, T1562.006, T1565 | TA0040  | M1029       |

## 6.2.2.5 Ensure rsyslog log file creation mode is configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

**rsyslog** will create logfiles that do not already exist on the system.

The **global()** configuration object **umask**, available in rsyslog 8.26.0+, sets the rsyslogd process' umask. If not specified, the system-provided default is used. The value given must always be a 4-digit octal number, with the initial digit being zero.

The legacy **\$umask** parameter sets the **rsyslogd** process' umask. If not specified, the system-provided default is used. The value given must always be a 4-digit octal number, with the initial digit being zero.

The legacy **\$FileCreateMode** parameter allows the setting of the mode with which **rsyslogd** creates new files. If not specified, the value **0644** is used. The value given must always be a 4-digit octal number, with the initial digit being zero. Please note that the actual permission depend on **rsyslogd** process **umask**. If in doubt, use **\$umask 0000** right at the beginning of the configuration file to remove any restrictions.

The legacy **\$FileCreateMode** may be specified multiple times. If so, it specifies the creation mode for all selector lines that follow until the next **\$FileCreateMode** parameter. Order of lines is vitally important.

### Rationale:

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

### Audit:

Run the following command

Run the following command to verify **\$FileCreateMode**:

```
# grep -Ps '^h*\$FileCreateMode\h+[0,2,4,6][0,2,4]0\b' /etc/rsyslog.conf  
/etc/rsyslog.d/*.conf
```

Verify the output is includes 0640 or more restrictive:

```
$FileCreateMode 0640
```

Should a site policy dictate less restrictive permissions, ensure to follow said policy.

**NOTE:** More restrictive permissions such as **0600** is implicitly sufficient.

## Remediation:

Edit either `/etc/rsyslog.conf` or a dedicated `.conf` file in `/etc/rsyslog.d/` and set `$FileCreateMode` to `0640` or more restrictive:

```
$FileCreateMode 0640
```

Restart the service:

```
# systemctl restart rsyslog
```

## References:

1. RSYSLOG.CONF(5)
2. NIST SP 800-53 Rev. 5: AC-3, AC-6, MP-2
3. <https://www.rsyslog.com/doc/>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |   |   |   |
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                                                                 |  |  |  |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                  |  |  |  |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.                                         |                                                                                       |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1083, T1083.000 | TA0007  | M1022       |

## 6.2.2.6 Ensure rsyslog logging is configured (Manual)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files specifies rules for logging and which files are to be used to log certain classes of messages.

### Rationale:

A great deal of important security-related information is sent via `rsyslog` (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

### Audit:

Review the contents of `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files to ensure appropriate logging is set. In addition, run the following command and verify that the log files are logging information as expected:

```
# ls -l /var/log/
```



## Remediation:

Edit the following lines in the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files as appropriate for your environment.

**Note:** The below configuration is shown for example purposes only. Due care should be given to how the organization wishes to store log data.

```
*.emerg                                :omusrmsg:*
auth,authpriv.*                       /var/log/secure
mail.*                                -/var/log/mail
mail.info                              -/var/log/mail.info
mail.warning                           -/var/log/mail.warn
mail.err                               /var/log/mail.err
cron.*                                /var/log/cron
*.=warning;*.=err                     -/var/log/warn
*.crit                                 /var/log/warn
*.*;mail.none;news.none               -/var/log/messages
local0,local1.*                       -/var/log/localmessages
local2,local3.*                       -/var/log/localmessages
local4,local5.*                       -/var/log/localmessages
local6,local7.*                       -/var/log/localmessages
```

Run the following command to reload the `rsyslogd` configuration:

```
# systemctl restart rsyslog
```

## References:

1. See the `rsyslog.conf(5)` man page for more information.
2. NIST SP 800-53 Rev. 5: AU-2, AU-7, AU-12

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                         |  |  |  |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          |  |  |  |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. |                                                                                       |  |  |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1070, T1070.002                   | TA0005         | M1047              |

## 6.2.2.7 Ensure rsyslog is configured to send logs to a remote log host (Manual)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

**rsyslog** supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralized log management.

### Rationale:

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

### Audit:

Review the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and verify that logs are sent to a central host:

#### basic format

```
# grep "^*.*[^\I][^\I]*@" /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Output should include `@@<FQDN or IP of remote loghost>`:

*Example:*

```
*.* @@loghost.example.com
```

#### advanced format

```
# grep -Psi -- '^\\s*([^\#]+\s+)?action\(([^\#]+\s+)?\btarget=\\\"?[^\#\"]+\\\"?\b' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Output should include `target=<FQDN or IP of remote loghost>`:

*Example:*

```
*.* action(type="omfwd" target="loghost.example.com" port="514" protocol="tcp")
```

## Remediation:

Edit the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and add the following line (where `loghost.example.com` is the name of your central log host). The `target` directive may either be a fully qualified domain name or an IP address.

*Example:*

```
*. * action(type="omfwd" target="loghost.example.com" port="514"
protocol="tcp"
        action.resumeRetryCount="100"
        queue.type="LinkedList" queue.size="1000")
```

Run the following command to reload `rsyslog.service`:

```
# systemctl reload-or-restart rsyslog.service
```

## References:

1. See the `rsyslog.conf(5)` man page for more information.
2. NIST SP 800-53 Rev. 5: AU-6
3. <https://www.rsyslog.com/doc/>

## Additional Information:

In addition, see the [rsyslog documentation](#) for implementation details of TLS.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                         |  |  |  |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          |  |  |  |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. |                                                                                       |  |  |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1070, T1070.002, T1562, T1562.006 | TA0040         | M1029              |

## 6.2.2.8 Ensure rsyslog is not configured to receive logs from a remote client (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

**rsyslog** supports the ability to receive messages from remote hosts, thus acting as a log server. Clients should not receive data from other hosts.

### Rationale:

If a client is configured to also receive data, thus turning it into a server, the client system is acting outside its operational boundary.

### Audit:

Review the **/etc/rsyslog.conf** and **/etc/rsyslog.d/\*.conf** files and verify that the system is not configured to accept incoming logs.

#### advanced format

```
# grep -Psi -- '^h*module\ (load= "\"?imtcp\ "\"?) ' /etc/rsyslog.conf
/etc/rsyslog.d/*.conf
# grep -Psi -- '^h*input\ (type= "\"?imtcp\ "\"?b' /etc/rsyslog.conf
/etc/rsyslog.d/*.conf
```

Nothing should be returned

#### obsolete legacy format

```
# grep -Psi -- '^h*${ModLoad}h+imtcp\b' /etc/rsyslog.conf
/etc/rsyslog.d/*.conf
# grep -Psi -- '^h*${InputTCPServerRun}\b' /etc/rsyslog.conf
/etc/rsyslog.d/*.conf
```

Nothing should be returned

## Remediation:

Should there be any active log server configuration found in the auditing section, modify those files and remove the specific lines highlighted by the audit. Verify none of the following entries are present in any of `/etc/rsyslog.conf` or `/etc/rsyslog.d/*.conf`.

### advanced format

```
module(load="imtcp")
input(type="imtcp" port="514")
```

### deprecated legacy format

```
$ModLoad imtcp
$InputTCPServerRun
```

Restart the service:

```
# systemctl restart rsyslog
```

## References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-7, AU-12, CM-6
2. <https://www.rsyslog.com/doc/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                       |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics        | Mitigations |
|------------------------------------|----------------|-------------|
| T1070, T1070.002, T1562, T1562.006 | TA0005, TA0040 | M1029       |

## 6.2.2.9 Ensure logrotate is configured (Manual)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The system includes the capability of rotating log files regularly to avoid filling up the system with logs or making the logs unmanageably large. The file `/etc/logrotate.d/syslog` is the configuration file used to rotate log files created by `syslog` or `rsyslog`.

### Rationale:

By keeping the log files smaller and more manageable, a system administrator can easily archive these files to another system and spend less time looking through inordinately large log files.

### Audit:

Review `/etc/logrotate.conf` and `/etc/logrotate.d/*` and verify logs are rotated according to site policy.

### Remediation:

Edit `/etc/logrotate.conf` and `/etc/logrotate.d/*` to ensure logs are rotated according to site policy.

### References:

1. NIST SP 800-53 Rev. 5: AU-8

### Additional Information:

If no `maxage` setting is set for `logrotate` a situation can occur where `logrotate` is interrupted and fails to delete rotated log files. It is recommended to set this to a value greater than the longest any log file should exist on your system to ensure that any such log file is removed but standard rotation settings are not overridden.



**CIS Controls:**

| Controls Version | Control                                                                                                                                                                  | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | 8.3 <u>Ensure Adequate Audit Log Storage</u><br>Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process. |  |  |  |
| v7               | 6.4 <u>Ensure adequate storage for logs</u><br>Ensure that all systems that store logs have adequate storage space for the logs generated.                               |                                                                                     |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1070, T1070.002            | TA0040  | M1022       |

### 6.2.2.10 Ensure rsyslog is configured to log cron events (Automated)

#### Profile Applicability:

- STIG

#### Description:

Cron logging must be implemented.

#### Rationale:

Cron logging can be used to trace the successful or unsuccessful execution of cron jobs. It can also be used to spot intrusions into the use of the cron facility by unauthorized and malicious users.

#### Audit:

Verify that "rsyslog" is configured to log cron events with the following command:  
Note: If another logging package is used, substitute the utility configuration file for "/etc/rsyslog.conf" or "/etc/rsyslog.d/\*.conf" files.

```
# grep -s cron /etc/rsyslog.conf /etc/rsyslog.d/*.conf

/etc/rsyslog.conf:*.info;mail.none;authpriv.none;cron.none /var/log/messages
/etc/rsyslog.conf:# Log cron stuff
/etc/rsyslog.conf:cron.* /var/log/cron
```

If the command does not return a response, check for cron logging all facilities with the following command.

```
# grep -s /var/log/messages /etc/rsyslog.conf /etc/rsyslog.d/*.conf

/etc/rsyslog.conf:*.info;mail.none;authpriv.none;cron.none /var/log/messages
```

If "rsyslog" is not logging messages for the cron facility or all facilities, this is a finding.

#### Remediation:

Configure "rsyslog" to log all cron messages by adding or updating the following line to "/etc/rsyslog.conf" or a configuration file in the /etc/rsyslog.d/ directory:

```
cron.* /var/log/cron
```

The rsyslog daemon must be restarted for the changes to take effect:

```
# systemctl restart rsyslog.service
```

#### References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230387  
Rule ID: SV-230387r743996  
STIG ID: RHEL-08-030010  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      |  |  |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.                                                                                |      |  |  |

### 6.2.2.11 *Ensure the rsyslog service is enabled and active (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The rsyslog service must be running.

#### **Rationale:**

Configuring the operating system to implement organization-wide security implementation guides and security checklists ensures compliance with federal standards and establishes a common security baseline across the DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

#### **Audit:**

Verify the rsyslog service is enabled and active with the following commands:

```
# systemctl is-enabled rsyslog
enabled

# systemctl is-active rsyslog
active
```

If the service is not "enabled" and "active" this is a finding.

#### **Remediation:**

Start the auditd service, and enable the rsyslog service with the following commands:

```
# systemctl start rsyslog.service
# systemctl enable rsyslog.service
```

#### **References:**

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230298  
Rule ID: SV-230298r627750  
STIG ID: RHEL-08-010561  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                | IG 1                                                                                | IG 2                                                                                 | IG 3                                                                                 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                         |  |   |   |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          |  |   |   |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. |                                                                                     |  |  |

## 6.2.2.12 Ensure the operating system has the packages required for encrypting offloaded audit logs (Automated)

### Profile Applicability:

- STIG

### Description:

must have the packages required for encrypting offloaded audit logs installed.

### Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

The operating system's installation media provides "rsyslogd". "rsyslogd" is a system utility providing support for message logging. Support for both internet and UNIX domain sockets enables this utility to support both local and remote logging. Couple this utility with "rsyslog-gnutls" (which is a secure communications library implementing the SSL, TLS and DTLS protocols), and you have a method to securely encrypt and off-load auditing.

Rsyslog provides three ways to forward message: the traditional UDP transport, which is extremely lossy but standard; the plain TCP based transport, which loses messages only during certain situations but is widely available; and the RELP transport, which does not lose messages but is currently available only as part of the rsyslogd 3.15.0 and above. Examples of each configuration: UDP . @remotesystemname TCP . @@remotesystemname RELP . :omrelp:remotesystemname:2514 Note that a port number was given as there is no standard port for RELP.

### Audit:

Verify the operating system has the packages required for encrypting offloaded audit logs installed with the following commands:

```
# yum list installed rsyslog-gnutls  
rsyslog-gnutls.x86_64 8.1911.0-3.el8 @AppStream
```

If the "rsyslog-gnutls" package is not installed, ask the administrator to indicate how audit logs are being encrypted during offloading and what packages are installed to support it. If there is no evidence of audit logs being encrypted during offloading, this is a finding.

## Remediation:

Configure the operating system to encrypt offloaded audit logs by installing the required packages with the following command:

```
# yum install rsyslog-gnutls
```

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230478  
Rule ID: SV-230478r744011  
STIG ID: RHEL-08-030680  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                              | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.9 <u>Centralize Audit Logs</u></b><br>Centralize, to the extent possible, audit log collection and retention across enterprise assets.                          |      | ●    | ●    |
| v7               | <b>6.6 <u>Deploy SIEM or Log Analytic tool</u></b><br>Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis. |      | ●    | ●    |

### 6.2.2.13 *Ensure the operating system authenticates the remote logging server for off-loading audit logs (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must authenticate the remote logging server for off-loading audit logs.

#### **Rationale:**

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

The operating system's installation media provides "rsyslogd". "rsyslogd" is a system utility providing support for message logging. Support for both internet and UNIX domain sockets enables this utility to support both local and remote logging. Couple this utility with "gnutls" (which is a secure communications library implementing the SSL, TLS and DTLS protocols), and you have a method to securely encrypt and off-load auditing.

"Rsyslog" supported authentication modes include: anon - anonymous authentication x509/fingerprint - certificate fingerprint authentication x509/certvalid - certificate validation only x509/name - certificate validation and subject name authentication.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

#### **Audit:**

Verify the operating system authenticates the remote logging server for off-loading audit logs with the following command:

```
# grep -i '$ActionSendStreamDriverAuthMode' /etc/rsyslog.conf
/etc/rsyslog.d/*.conf

/etc/rsyslog.conf:$ActionSendStreamDriverAuthMode x509/name
```

If the value of the "\$ActionSendStreamDriverAuthMode" option is not set to "x509/name" or the line is commented out, ask the System Administrator to indicate how the audit logs are off-loaded to a different system or media.

If there is no evidence that the transfer of the audit logs being off-loaded to another system or media is encrypted, this is a finding.



**Remediation:**

Configure the operating system to authenticate the remote logging server for off-loading audit logs by setting the following option in "/etc/rsyslog.conf" or "/etc/rsyslog.d/[customfile].conf":

```
$ActionSendStreamDriverAuthMode x509/name
```

**References:**

- 1. NIST SP 800-53 Revision 5 :: AU-4 (1)

**Additional Information:**

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230482  
Rule ID: SV-230482r877390  
STIG ID: RHEL-08-030720  
Severity: CAT II

**CIS Controls:**

| Controls Version | Control                                                                                                                                                       | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | 8.9 <u>Centralize Audit Logs</u><br>Centralize, to the extent possible, audit log collection and retention across enterprise assets.                          |      |  |  |
| v7               | 6.6 <u>Deploy SIEM or Log Analytic tool</u><br>Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis. |      |  |  |

#### *6.2.2.14 Ensure the operating system encrypts audit records off-loaded onto a different system or media from the system being audited (Automated)*

##### **Profile Applicability:**

- STIG

##### **Description:**

The operating system must encrypt the transfer of audit records off-loaded onto a different system or media from the system being audited.

##### **Rationale:**

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

The operating system's installation media provides "rsyslogd". "rsyslogd" is a system utility providing support for message logging. Support for both internet and UNIX domain sockets enables this utility to support both local and remote logging. Couple this utility with "gnutls" (which is a secure communications library implementing the SSL, TLS and DTLS protocols), and you have a method to securely encrypt and off-load auditing.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

## Audit:

Verify the operating system encrypts audit records off-loaded onto a different system or media from the system being audited with the following commands:

```
# grep -i '$DefaultNetstreamDriver' /etc/rsyslog.conf /etc/rsyslog.d/*.conf  
  
/etc/rsyslog.conf:$DefaultNetstreamDriver gtls
```

If the value of the "\$DefaultNetstreamDriver" option is not set to "gtls" or the line is commented out, this is a finding.

```
# grep -i '$ActionSendStreamDriverMode' /etc/rsyslog.conf  
/etc/rsyslog.d/*.conf  
  
/etc/rsyslog.conf:$ActionSendStreamDriverMode 1
```

If the value of the "\$ActionSendStreamDriverMode" option is not set to "1" or the line is commented out, this is a finding.

If either of the definitions above are set, ask the System Administrator to indicate how the audit logs are off-loaded to a different system or media.

If there is no evidence that the transfer of the audit logs being off-loaded to another system or media is encrypted, this is a finding.

## Remediation:

Configure the operating system to encrypt off-loaded audit records by setting the following options in "/etc/rsyslog.conf" or "/etc/rsyslog.d/[customfile].conf":

```
$DefaultNetstreamDriver gtls  
$ActionSendStreamDriverMode 1
```

## References:

1. NIST SP 800-53 Revision 5 :: AU-4 (1)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230481  
Rule ID: SV-230481r877390  
STIG ID: RHEL-08-030710  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                              | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.9 <u>Centralize Audit Logs</u></b><br>Centralize, to the extent possible, audit log collection and retention across enterprise assets.                          |      | ●    | ●    |
| v7               | <b>6.6 <u>Deploy SIEM or Log Analytic tool</u></b><br>Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis. |      | ●    | ●    |

### *6.2.2.15 Ensure the audit system off-loads audit records onto a different system or media from the system being audited (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Audit records must be off-loaded onto a different system or storage media from the system being audited.

#### **Rationale:**

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

The operating system's installation media provides "rsyslogd". "rsyslogd" is a system utility providing support for message logging. Support for both internet and UNIX domain sockets enables this utility to support both local and remote logging. Couple this utility with "gnutls" (which is a secure communications library implementing the SSL, TLS and DTLS protocols), and you have a method to securely encrypt and off-load auditing.

Rsyslog provides three ways to forward message: the traditional UDP transport, which is extremely lossy but standard; the plain TCP based transport, which loses messages only during certain situations but is widely available; and the RELP transport, which does not lose messages but is currently available only as part of the rsyslogd 3.15.0 and above. Examples of each configuration: UDP . @remotesystemname TCP . @@remotesystemname RELP . :omrelp:remotesystemname:2514 Note that a port number was given as there is no standard port for RELP.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

## Audit:

Verify the audit system off-loads audit records onto a different system or media from the system being audited with the following command:

```
# grep @@ /etc/rsyslog.conf /etc/rsyslog.d/*.conf  
  
/etc/rsyslog.conf:*. * @@[remoteloggingserver]:[port]
```

If a remote server is not configured, or the line is commented out, ask the System Administrator to indicate how the audit logs are off-loaded to a different system or media.

If there is no evidence that the audit logs are being off-loaded to another system or media, this is a finding.

## Remediation:

Configure the operating system to off-load audit records onto a different system or media from the system being audited by specifying the remote logging server in "/etc/rsyslog.conf" or "/etc/rsyslog.d/[customfile].conf" with the name or IP address of the log aggregation server.

```
*.* @@[remoteloggingserver]:[port]
```

## References:

1. NIST SP 800-53 Revision 5 :: AU-4 (1)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230479  
Rule ID: SV-230479r917883  
STIG ID: RHEL-08-030690  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                       | IG 1 | IG 2 | IG 3 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.9 Centralize Audit Logs</b><br>Centralize, to the extent possible, audit log collection and retention across enterprise assets.                          |      | ●    | ●    |
| v7               | <b>6.6 Deploy SIEM or Log Analytic tool</b><br>Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis. |      | ●    | ●    |

### 6.2.3 Configure Logfiles

### *6.2.3.1 Ensure access to all logfiles has been configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Log files contain information from many services on the the local system, or in the event of a centralized log server, others systems logs as well.

In general log files are found in `/var/log/`, although application can be configured to store logs elsewhere. Should your application store logs in another, ensure to run the same test on that location.

#### **Rationale:**

It is important that log files have the correct permissions to ensure that sensitive data is protected and that only the appropriate users / groups have access to them.

#### **Audit:**

Run the following script to verify that files in `/var/log/` have appropriate permissions and ownership:



```

#!/usr/bin/env bash

{
    a_output=(); a_output2=()
    f_file_test_chk()
    {
        a_out2=()
        maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
        [ $(( $l_mode & $perm_mask )) -gt 0 ] && \
            a_out2+=("    o Mode: \"$l_mode\" should be \"$maxperm\" or more
restrictive")
        [[ ! "$l_user" =~ $l_auser ]] && \
            a_out2+=("    o Owned by: \"$l_user\" and should be owned by
\"${l_auser}[/|/ or ]\"")
        [[ ! "$l_group" =~ $l_agroup ]] && \
            a_out2+=("    o Group owned by: \"$l_group\" and should be group
owned by \"${l_agroup}[/|/ or ]\"")
        [ "${a_out2[@]}" -gt 0 ] && a_output2+=(" - File: \"$l_fname\" is:"
"${a_out2[@]}")
    }
    while IFS= read -r -d $'\0' l_file; do
        while IFS=: read -r l_fname l_mode l_user l_group; do
            if grep -Pq -- '\/(apt)\h*$' <<< "$(dirname "$l_fname")"; then
                perm_mask='0133' l_auser="root" l_agroup="(root|adm)";
f_file_test_chk
            else
                case "$(basename "$l_fname")" in
                    lastlog | lastlog.* | wtmp | wtmp.* | wtmp-* | btmp | btmp.* |
btmp-* | README)
                        perm_mask='0113' l_auser="root" l_agroup="(root|utmp)"
                        f_file_test_chk ;;
                    cloud-init.log* | localmessages* | waagent.log*)
                        perm_mask='0133' l_auser="(root|syslog)"
l_agroup="(root|adm)"
                        file_test_chk ;;
                    secure{,*,*,*,*} | auth.log | syslog | messages)
                        perm_mask='0137' l_auser="(root|syslog)"
l_agroup="(root|adm)"
                        f_file_test_chk ;;
                    SSSD | sssd)
                        perm_mask='0117' l_auser="(root|SSSD)"
l_agroup="(root|SSSD)"
                        f_file_test_chk ;;
                    gdm | gdm3)
                        perm_mask='0117' l_auser="root" l_agroup="(root|gdm|gdm3)"
                        f_file_test_chk ;;
                    *.journal | *.journal~)
                        perm_mask='0137' l_auser="root" l_agroup="(root|systemd-
journal)"
                        f_file_test_chk ;;
                    *)
                        perm_mask='0137' l_auser="(root|syslog)"
l_agroup="(root|adm)"
                        if [ "$l_user" = "root" ] || ! grep -Pq -- "^h*$"$(awk -F:
'$1=="'"$l_user"'"' {print $7}' /etc/passwd)\b' /etc/shells; then
                            ! grep -Pq -- "$l_auser" <<< "$l_user" &&
l_auser="(root|syslog|$l_user)"

```

```

        ! grep -Pq -- "$l_agroup" <<< "$l_group" &&
l_agroup="(root|adm|$l_group)"
        fi
        f_file_test_chk ;;
    esac
fi
done < <(stat -Lc '%n:%#a:%U:%G' "$l_file")
done < <(find -L /var/log -type f \( -perm /0137 -o ! -user root -o ! -
group root \) -print0)
if [ "${#a_output2[@]}" -le 0 ]; then
    a_output+=(" - All files in \"/var/log/" have appropriate permissions
and ownership")
    printf '\n%s' "- Audit Result:" " ** PASS **" "${a_output[@]}" ""
else
    printf '\n%s' "- Audit Result:" " ** FAIL **" " - Reason(s) for audit
failure:" "${a_output2[@]}" ""
fi
}

```

### Remediation:

Run the following script to update permissions and ownership on files in **/var/log**. Although the script is not destructive, ensure that the output is captured in the event that the remediation causes issues.

```

#!/usr/bin/env bash

{
    a_output2=()
    f_file_test_fix()
    {
        a_out2=()
        maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
        if [ $(( $l_mode & $perm_mask )) -gt 0 ]; then
            a_out2+=("    o Mode: \"$l_mode\" should be \"$maxperm\" or more
restrictive" "          x Removing excess permissions")
            chmod "$l_rperms" "$l_fname"
        fi
        if [[ ! "$l_user" =~ $l_auser ]]; then
            a_out2+=("    o Owned by: \"$l_user\" and should be owned by
\"${l_auser}/// or }\" "          x Changing ownership to: \"$l_fix_account\")
            chown "$l_fix_account" "$l_fname"
        fi
        if [[ ! "$l_group" =~ $l_agroup ]]; then
            a_out2+=("    o Group owned by: \"$l_group\" and should be group
owned by \"${l_agroup}/// or }\" "          x Changing group ownership to:
\"$l_fix_account\")
            chgrp "$l_fix_account" "$l_fname"
        fi
        [ "${#a_out2[@]}" -gt 0 ] && a_output2+=(" - File: \"$l_fname\" is:"
"${a_out2[@]}")
    }
    l_fix_account='root'
    while IFS= read -r -d $'\0' l_file; do
        while IFS=: read -r l_fname l_mode l_user l_group; do
            if grep -Pq -- '\/(apt)\h*$' <<< "$(dirname "$l_fname")"; then
                perm_mask='0133' l_rperms="u-x,go-wx" l_auser="root"
            l_agroup="(root|adm)"; f_file_test_fix
            else
                case "$(basename "$l_fname")" in
                    lastlog | lastlog.* | wtmp | wtmp.* | wtmp-* | btmp | btmp.* |
btmp-* | README)
                        perm_mask='0113' l_rperms="ug-x,o-wx" l_auser="root"
                    l_agroup="(root|utmp)"
                        f_file_test_fix ;;
                    cloud-init.log* | localmessages* | waagent.log*)
                        perm_mask='0133' l_rperms="u-x,go-wx"
                    l_auser="(root|syslog)" l_agroup="(root|adm)"
                        file_test_fix ;;
                    secure | auth.log | syslog | messages)
                        perm_mask='0137' l_rperms="u-x,g-wx,o-rwx"
                    l_auser="(root|syslog)" l_agroup="(root|adm)"
                        f_file_test_fix ;;
                    SSSD | sssd)
                        perm_mask='0117' l_rperms="ug-x,o-rwx"
                    l_auser="(root|SSSD)" l_agroup="(root|SSSD)"
                        f_file_test_fix ;;
                    gdm | gdm3)
                        perm_mask='0117' l_rperms="ug-x,o-rwx" l_auser="root"
                    l_agroup="(root|gdm|gdm3)"
                        f_file_test_fix ;;
                    *.journal | *.journal~)

```

```

        perm_mask='0137' l_rperms="u-x,g-wx,o-rwx" l_auser="root"
l_agroup="(root|systemd-journal)"
        f_file_test_fix ;;
    *)
        perm_mask='0137' l_rperms="u-x,g-wx,o-rwx"
l_auser="(root|syslog)" l_agroup="(root|adm)"
        if [ "$l_user" = "root" ] || ! grep -Pq -- "^\h*$" (awk -F:
'$1=="'"$l_user"'"' {print $7}' /etc/passwd)\b" /etc/shells; then
            ! grep -Pq -- "$l_auser" <<< "$l_user" &&
l_auser="(root|syslog|$l_user)"
            ! grep -Pq -- "$l_agroup" <<< "$l_group" &&
l_agroup="(root|adm|$l_group)"
        fi
        f_file_test_fix ;;
    esac
fi
done < <(stat -Lc '%n:%a:%U:%G' "$l_file")
done < <(find -L /var/log -type f \( -perm /0137 -o ! -user root -o ! -
group root \) -print0)
if [ "${#a_output2[@]}" -le 0 ]; then # If all files passed, then we
report no changes
    a_output+="( - All files in \"/var/log/" have appropriate permissions
and ownership)"
    printf '\n%s' "- All files in \"/var/log/" have appropriate
permissions and ownership" " o No changes required" ""
else
    printf '\n%s' "${a_output2[@]}" ""
fi
}

```

**Note:** You may also need to change the configuration for your logging software or services for any logs that had incorrect permissions.

If there are services that log to other locations, ensure that those log files have the appropriate access configured.

## References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1083, T1083.000 | TA0007  | M1028       |

### 6.2.3.2 Ensure /var/log/messages mode is configured (Automated)

#### Profile Applicability:

- STIG

#### Description:

The "/var/log/messages" file must have mode "0640" or less permissive.

#### Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

#### Audit:

Verify that the "/var/log/messages" file has mode "0640" or less permissive with the following command:

```
# stat -c "%a %n" /var/log/messages  
640 /var/log/messages
```

If a value of "0640" or less permissive is not returned, this is a finding.

#### Remediation:

Change the permissions of the file "/var/log/messages" to "0640" by running the following command:

```
# chmod 0640 /var/log/messages
```

#### References:

1. NIST SP 800-53 Revision 5 :: SI-11 b
2. NIST SP 800-53A :: SI-11.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230245  
Rule ID: SV-230245r627750  
STIG ID: RHEL-08-010210  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### 6.2.3.3 Ensure /var/log/messages owner is configured (Automated)

#### Profile Applicability:

- STIG

#### Description:

The "/var/log/messages" file must be owned by root.

#### Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

#### Audit:

Verify that the "/var/log/messages" file is owned by root with the following command:

```
# stat -c "%U" /var/log/messages  
root
```

If "root" is not returned as a result, this is a finding.

#### Remediation:

Change the owner of the file /var/log/messages to root by running the following command:

```
# chown root /var/log/messages
```

#### References:

1. NIST SP 800-53 Revision 5 :: SI-11 b
2. NIST SP 800-53A :: SI-11.1 (iv)



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230246  
Rule ID: SV-230246r627750  
STIG ID: RHEL-08-010220  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### 6.2.3.4 Ensure /var/log/messages group owner is configured (Automated)

#### Profile Applicability:

- STIG

#### Description:

The "/var/log/messages" file must be group-owned by root.

#### Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

#### Audit:

Verify the "/var/log/messages" file is group-owned by root with the following command:

```
# stat -c "%G" /var/log/messages  
root
```

If "root" is not returned as a result, this is a finding.

#### Remediation:

Change the group of the file "/var/log/messages" to "root" by running the following command:

```
# chgrp root /var/log/messages
```

#### References:

1. NIST SP 800-53 Revision 5 :: SI-11 b
2. NIST SP 800-53A :: SI-11.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230247  
Rule ID: SV-230247r627750  
STIG ID: RHEL-08-010230  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### 6.2.3.5 Ensure /var/log is mode is configured (Automated)

#### Profile Applicability:

- STIG

#### Description:

The "/var/log" directory must have mode 0755 or less permissive.

#### Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

#### Audit:

Verify that the "/var/log" directory has a mode of "0755" or less with the following command:

```
# stat -c "%a %n" /var/log  
  
755
```

If a value of "0755" or less permissive is not returned, this is a finding.

#### Remediation:

Change the permissions of the directory "/var/log" to "0755" by running the following command:

```
# chmod 0755 /var/log
```

#### References:

1. NIST SP 800-53 Revision 5 :: SI-11 b
2. NIST SP 800-53A :: SI-11.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230248  
Rule ID: SV-230248r627750  
STIG ID: RHEL-08-010240  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### 6.2.3.6 Ensure /var/log owner is configured (Automated)

#### Profile Applicability:

- STIG

#### Description:

The "/var/log" directory must be owned by root.

#### Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

#### Audit:

Verify the "/var/log" directory is owned by root with the following command:

```
# stat -c "%U" /var/log  
root
```

If "root" is not returned as a result, this is a finding.

#### Remediation:

Change the owner of the directory "/var/log" to root by running the following command:

```
# chown root /var/log
```

#### References:

1. NIST SP 800-53 Revision 5 :: SI-11 b
2. NIST SP 800-53A :: SI-11.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230249  
Rule ID: SV-230249r627750  
STIG ID: RHEL-08-010250  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### 6.2.3.7 Ensure /var/log group owner is configured (Automated)

#### Profile Applicability:

- STIG

#### Description:

The "/var/log" directory must be group-owned by root.

#### Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

#### Audit:

Verify the "/var/log" directory is group-owned by root with the following command:

```
# stat -c "%G" /var/log
root
```

If "root" is not returned as a result, this is a finding.

#### Remediation:

Change the group of the directory "/var/log" to "root" by running the following command:

```
# chgrp root /var/log
```

#### References:

1. NIST SP 800-53 Revision 5 :: SI-11 b
2. NIST SP 800-53A :: SI-11.1 (iv)



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230250  
Rule ID: SV-230250r627750  
STIG ID: RHEL-08-010260  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### *6.2.3.8 Ensure administrators are notified if an audit processing failure occurs by modifying /etc/aliases (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system's Information System Security Officer (ISSO) and System Administrator (SA) (at a minimum) must have mail aliases to be notified of an audit processing failure.

#### **Rationale:**

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

#### **Audit:**

Verify that the administrators are notified in the event of an audit processing failure. Check that the "/etc/aliases" file has a defined value for "root".

```
# grep "postmaster:\s*root$" /etc/aliases
```

If the command does not return a line, or the line is commented out, ask the system administrator to indicate how they and the ISSO are notified of an audit process failure. If there is no evidence of the proper personnel being notified of an audit processing failure, this is a finding.

#### **Remediation:**

Configure the operating system to notify administrators in the event of an audit processing failure.

Add/update the following line in "/etc/aliases":

```
postmaster: root
```

#### **References:**

1. NIST SP 800-53 :: AU-5 a
2. NIST SP 800-53A :: AU-5.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230389  
Rule ID: SV-230389r627750  
STIG ID: RHEL-08-030030  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  |  |  |  |

## 6.3 System Auditing

The Linux Auditing System operates on a set of rules that collects certain types of system activity to facilitate incident investigation, detect unauthorized access or modification of data. By default events will be logged to `/var/log/audit/audit.log`, which can be configured in `/etc/audit/auditd.conf`.

The following types of audit rules can be specified:

- Control rules: Configuration of the auditing system.
- File system rules: Allow the auditing of access to a particular file or a directory. Also known as file watches.
- System call rules: Allow logging of system calls that any specified program makes.

Audit rules can be set:

- On the command line using the `auditctl` utility. These rules are not persistent across reboots.
- In `/etc/audit/audit.rules`. These rules have to be merged and loaded before they are active.

### Note:

- For 64 bit systems that have `arch` as a rule parameter, you will need two rules: one for 64 bit and one for 32 bit systems calls. For 32 bit systems, only one rule is needed.
- If the auditing system is configured to be locked (`-e 2`), a system reboot will be required in order to load any changes.
- Key names are optional on the rules and will not be used in compliance auditing. The usage of key names is highly recommended as it facilitates organization and searching; as such, all remediation steps will have key names supplied.
- It is best practice to store the rules, in number prepended files, in `/etc/audit/rules.d/`. Rules must end in a `.rules` suffix. This then requires the use of `augenrules` to merge all the rules into `/etc/audit/audit.rules` based on their alphabetical (lexical) sort order. All benchmark recommendations follow this best practice for remediation, specifically using the prefix of `50` which is center weighed if all rule sets make use of the number prepending naming convention.
- Your system may have been customized to change the default `UID_MIN`. All sample output uses `1000`, but this value will not be used in compliance auditing. To confirm the `UID_MIN` for your system, run the following command: `awk '/^s*UID_MIN/{print $2}' /etc/login.defs`

**Normalization** The Audit system normalizes some entries, so when you look at the sample output keep in mind that:

- With regards to users whose login UID is not set, the values **-1** / **unset** / **4294967295** are equivalent and normalized to **-1**.
- When comparing field types and both sides of the comparison is valid fields types, such as **euid!=uid**, then the auditing system may normalize such that the output is **uid!=euid**.
- Some parts of the rule may be rearranged whilst others are dependent on previous syntax. For example, the following two statements are the same:

```
-a always,exit -F arch=b64 -S execve -C uid!=euid -F auid!=-1 -F  
key=user_emulation
```

and

```
-a always,exit -F arch=b64 -C euid!=uid -F auid!=unset -S execve -k  
user_emulation
```

## Capacity planning

The recommendations in this section implement auditing policies that not only produce large quantities of logged data, but may also negatively impact system performance. Capacity planning is critical in order not to adversely impact production environments.

- **Disk space.** If a significantly large set of events are captured, additional on system or off system storage may need to be allocated. If the logs are not sent to a remote log server, ensure that log rotation is implemented else the disk will fill up and the system will halt. Even when logs are sent to a log server, ensure sufficient disk space to allow caching of logs in the case of temporary network outages.
- **Disk IO.** It is not just the amount of data collected that should be considered, but the rate at which logs are generated.
- **CPU overhead.** System call rules might incur considerable CPU overhead. Test the systems open/close syscalls per second with and without the rules to gauge the impact of the rules.

### **6.3.1 Configure auditd Service**

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

### 6.3.1.1 Ensure auditd packages are installed (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### Description:

**auditd** is the userspace component to the Linux Auditing System. It's responsible for writing audit records to the disk.

#### Rationale:

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000040-GPOS-00018, SRG-OS-000041-GPOS-00019, SRG-OS-000042-GPOS-00021, SRG-OS-000051-GPOS-00024, SRG-OS-000054-GPOS-00025, SRG-OS-000122-GPOS-00063, SRG-OS-000254-GPOS-00095, SRG-OS-000255-GPOS-00096, SRG-OS-000337-GPOS-00129, SRG-OS-000348-GPOS-00136, SRG-OS-000349-GPOS-00137, SRG-OS-000350-GPOS-00138, SRG-OS-000351-GPOS-00139, SRG-OS-000352-GPOS-00140, SRG-OS-000353-GPOS-00141, SRG-OS-000354-GPOS-00142, SRG-OS-000358-GPOS-00145, SRG-OS-000365-GPOS-00152, SRG-OS-000392-GPOS-00172, SRG-OS-000475-GPOS-00220

#### Audit:

Run the following command and verify **audit** and **audit-libs** packages are installed:

```
# rpm -q audit audit-libs  
  
audit-<version>  
audit-libs-<version>
```

#### Remediation:

Run the following command to install **audit** and **audit-libs**:

```
# dnf install audit audit-libs
```

#### References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-3, AU-3(1), AU-12, SI-5
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230411  
Rule ID: SV-230411r744000  
STIG ID: RHEL-08-030180  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.2 Collect Audit Logs</b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                                                                                                        |    |    |    |
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |                                                                                       |    |    |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         |  |  |  |
| v7               | <b>6.3 Enable Detailed Logging</b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.                                                                                |                                                                                       |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.001            | TA0005  | M1022       |



### 6.3.1.2 Ensure auditing for processes that start prior to auditd is enabled (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### Description:

Configure **grub2** so that processes that are capable of being audited can be audited even if they start up prior to **auditd** startup.

#### Rationale:

Audit events need to be captured on processes that start up prior to **auditd** , so that potential malicious activity cannot go undetected.

#### Audit:

**Note:** **/etc/default/grub** should be checked because the **grub2-mkconfig -o** command will overwrite **grub.cfg** with parameters listed in **/etc/default/grub**. Run the following command to verify that the **audit=1** parameter has been set:

```
# grubby --info=ALL | grep -Po '\baudit=1\b'

audit=1
```

**Note:** **audit=1** may be returned multiple times

Run the following command to verify that the **audit=1** parameter has been set in **/etc/default/grub**:

```
# grep -Psoi -- '^\\h*GRUB_CMDLINE_LINUX=\"([^\n\r]+\\h+)?audit=1\b'
/etc/default/grub
```

#### Example output:

```
GRUB_CMDLINE_LINUX="quiet audit=1"
```

**Note:** Other parameters may also be listed

## Remediation:

Run the following command to update the **grub2** configuration with **audit=1**:

```
# grubby --update-kernel ALL --args 'audit=1'
```

Edit **/etc/default/grub** and add **audit=1** to the **GRUB\_CMDLINE\_LINUX=** line between the opening and closing double quotes:

*Example:*

```
GRUB_CMDLINE_LINUX="quiet audit=1"
```

**Note:** Other parameters may also be listed

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230468  
Rule ID: SV-230468r792904  
STIG ID: RHEL-08-030601  
Severity: CAT III

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000473-GPOS-00218

This recommendation is designed around the grub 2 bootloader, if another bootloader is in use in your environment enact equivalent settings.

**grubby** is a command line tool used to configure bootloader menu entries across multiple architectures. It is used for updating and displaying information about the configuration files for various architecture specific bootloaders.

It is primarily designed to be used from scripts which install new kernels and need to find information about the current boot environment.

The grubby executable has full support for the grub2 bootloader on x86\_64 systems using legacy BIOS or modern UEFI firmware and ppc64 and ppc64le hardware using OPAL or SLOF as firmware.

Legacy s390 and the current s390x architectures and their zipl bootloader are fully supported.

Support for yaboot has been deprecated as all ppc architecture hardware since the Power8 uses grub2 or petitboot which both use the grub2 configuration file format.

Legacy bootloaders LILO, SILO, and ELILO are deprecated and no longer receiving active support in favor of previously mentioned bootloaders.

The default bootloader target is primarily determined by the architecture for which grubby has been built. Each architecture has a preferred bootloader, and each bootloader has its own configuration file. If no bootloader is selected on the command line, grubby will use these default settings to search for an existing configuration. If no bootloader configuration file is found, grubby will use the default value for that architecture.

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  |  |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.001            | TA0005  |             |

### 6.3.1.3 Ensure audit\_backlog\_limit is sufficient (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

#### Description:

The `audit_backlog_limit` parameter determines how auditd records can be held in the auditd backlog. The default setting of 64 may be insufficient to store all audit events during boot.

#### Rationale:

During boot if `audit=1`, then the backlog will hold 64 records. If more than 64 records are created during boot, auditd records will be lost and potential malicious activity could go undetected.

#### Audit:

**Note:** `/etc/default/grub` should be checked because the `grub2-mkconfig -o` command will overwrite `grub.cfg` with parameters listed in `/etc/default/grub`. Run the following command and verify the `audit_backlog_limit=` parameter is set to an appropriate size for your organization

```
# grubby --info=ALL | grep -Po "\baudit_backlog_limit=\d+\b"
audit_backlog_limit=<BACKLOG SIZE>
```

Validate that the line(s) returned contain a value for `audit_backlog_limit=` that is sufficient for your organization.

**Recommended that this value be 8192 or larger.**

Run the following command to verify that the `audit_backlog_limit=<BACKLOG SIZE>` parameter has been set in `/etc/default/grub`:

```
# grep -Psoi --
'^\h*GRUB_CMDLINE_LINUX=\"([^\n\r]+\h+)?\baudit_backlog_limit=\d+\b'
/etc/default/grub
```

#### Example output:

```
GRUB_CMDLINE_LINUX="quiet audit_backlog_limit=8192"
```

**Note:** Other parameters may also be listed

## Remediation:

Run the following command to add `audit_backlog_limit=<BACKLOG SIZE>` to `GRUB_CMDLINE_LINUX`:

```
# grubby --update-kernel ALL --args 'audit_backlog_limit=<BACKLOG SIZE>'
```

*Example:*

```
# grubby --update-kernel ALL --args 'audit_backlog_limit=8192'
```

Edit `/etc/default/grub` and add `audit_backlog_limit=<BACKLOG SIZE>` to the `GRUB_CMDLINE_LINUX=` line between the opening and closing double quotes:

*Example:*

```
GRUB_CMDLINE_LINUX="quiet audit_backlog_limit=8192"
```

**Note:** Other parameters may also be listed

## References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-12, SI-5

## Additional Information:

This recommendation is designed around the grub 2 bootloader, if another bootloader is in use in your environment enact equivalent settings.

**grubby** is a command line tool used to configure bootloader menu entries across multiple architectures. It is used for updating and displaying information about the configuration files for various architecture specific bootloaders.

It is primarily designed to be used from scripts which install new kernels and need to find information about the current boot environment.

The grubby executable has full support for the grub2 bootloader on x86\_64 systems using legacy BIOS or modern UEFI firmware and ppc64 and ppc64le hardware using OPAL or SLOF as firmware.

Legacy s390 and the current s390x architectures and their zipl bootloader are fully supported.

Support for yaboot has been deprecated as all ppc architecture hardware since the Power8 uses grub2 or petitboot which both use the grub2 configuration file format.

Legacy bootloaders LILO, SILO, and ELILO are deprecated and no longer receiving active support in favor of previously mentioned bootloaders.

The default bootloader target is primarily determined by the architecture for which grubby has been built. Each architecture has a preferred bootloader, and each bootloader has its own configuration file. If no bootloader is selected on the command line, grubby will use these default settings to search for an existing configuration. If no bootloader configuration file is found, grubby will use the default value for that architecture.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  |  |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.001            | TA0005  |             |



### 6.3.1.4 Ensure auditd service is enabled and active (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### Description:

Turn on the **auditd** daemon to record system events.

#### Rationale:

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

#### Audit:

Run the following command to verify **auditd** is enabled:

```
# systemctl is-enabled auditd | grep '^enabled'
enabled
```

Verify result is "enabled".

Run the following command to verify **auditd** is active:

```
# systemctl is-active auditd | grep '^active'
active
```

Verify result is active

#### Remediation:

Run the following commands to unmask, enable and start **auditd**:

```
# systemctl unmask auditd
# systemctl enable auditd
# systemctl start auditd
```

#### References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244542  
Rule ID: SV-244542r818838  
STIG ID: RHEL-08-030181  
Severity: CAT II

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000040-GPOS-00018, SRG-OS-000041-GPOS-00019, SRG-OS-000042-GPOS-00021, SRG-OS-000051-GPOS-00024, SRG-OS-000054-GPOS-00025, SRG-OS-000122-GPOS-00063, SRG-OS-000254-GPOS-00095, SRG-OS-000255-GPOS-00096, SRG-OS-000337-GPOS-00129, SRG-OS-000348-GPOS-00136, SRG-OS-000349-GPOS-00137, SRG-OS-000350-GPOS-00138, SRG-OS-000351-GPOS-00139, SRG-OS-000352-GPOS-00140, SRG-OS-000353-GPOS-00141, SRG-OS-000354-GPOS-00142, SRG-OS-000358-GPOS-00145, SRG-OS-000365-GPOS-00152, SRG-OS-000392-GPOS-00172, SRG-OS-000475-GPOS-00220

Additional methods of enabling a service exist. Consult your distribution documentation for appropriate methods.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                         |  |  |  |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                          |  |  |  |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements. |                                                                                       |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.001            | TA0005  |             |

### *6.3.1.5 Ensure the operating system allocates a sufficient audit\_backlog\_limit to capture processes that start prior to the audit daemon (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must allocate an audit\_backlog\_limit of sufficient size to capture processes that start prior to the audit daemon.

#### **Rationale:**

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

If auditing is enabled late in the startup process, the actions of some startup processes may not be audited. Some audit systems also maintain state information only available if auditing is enabled before a given process is created.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Allocating an audit\_backlog\_limit of sufficient size is critical in maintaining a stable boot process. With an insufficient limit allocated, the system is susceptible to boot failures and crashes.

#### **Audit:**

Verify the operating system allocates a sufficient audit\_backlog\_limit to capture processes that start prior to the audit daemon with the following commands:

```
# grub2-editenv - list | grep audit

kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto
resume=/dev/mapper/rhel-swap rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap rhgb
quiet fips=1 audit=1 audit_backlog_limit=8192 boot=UUID=8d171156-cd61-421c-
ba41-1c021ac29e82
```

If the "audit\_backlog\_limit" entry does not equal "8192" or greater, is missing, or the line is commented out, this is a finding.

Check the audit\_backlog\_limit is set to persist in kernel updates:

```
# grep audit /etc/default/grub

GRUB_CMDLINE_LINUX="audit_backlog_limit=8192"
```

If "audit\_backlog\_limit" is not set to "8192" or greater, is missing or commented out, this is a finding.

## Remediation:

Configure the operating system to allocate sufficient `audit_backlog_limit` to capture processes that start prior to the audit daemon with the following command:

```
# grubby --update-kernel=ALL --args="audit_backlog_limit=8192"
```

Add or modify the following line in `/etc/default/grub` to ensure the configuration survives kernel updates:

```
GRUB_CMDLINE_LINUX="audit_backlog_limit=8192"
```

## References:

1. NIST SP 800-53 Revision 5 :: AU-4

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230469  
Rule ID: SV-230469r877391  
STIG ID: RHEL-08-030602  
Severity: CAT III

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.                                                                                |      | ●    | ●    |

### *6.3.1.6 Ensure the operating system's audit daemon is configured to include local events (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The audit system must audit local events.

#### **Rationale:**

Without establishing what type of events occurred, the source of events, where events occurred, and the outcome of events, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

#### **Audit:**

Verify the the operating system's audit daemon is configured to include local events, with the following command:

```
# grep local_events /etc/audit/auditd.conf  
  
local_events = yes
```

If the value of the "local\_events" option is not set to "yes", or the line is commented out, this is a finding.

#### **Remediation:**

Configure the operating system to audit local events on the system.  
Add or update the following line in "/etc/audit/auditd.conf" file:

```
local_events = yes
```

#### **References:**

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230393  
Rule ID: SV-230393r627750  
STIG ID: RHEL-08-030061  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

### *6.3.1.7 Ensure the operating system's audit daemon is configured to label all off-loaded audit logs (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must label all off-loaded audit logs before sending them to the central log server.

#### **Rationale:**

Without establishing what type of events occurred, the source of events, where events occurred, and the outcome of events, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Enriched logging is needed to determine who, what, and when events occur on a system. Without this, determining root cause of an event will be much more difficult.

When audit logs are not labeled before they are sent to a central log server, the audit data will not be able to be analyzed and tied back to the correct system.

#### **Audit:**

Verify the operating system's audit daemon is configured to label all off-loaded audit logs, with the following command:

```
# grep "name_format" /etc/audit/auditd.conf  
name_format = hostname
```

If the "name\_format" option is not "hostname", "fqd", or "numeric", or the line is commented out, this is a finding.

#### **Remediation:**

Edit the /etc/audit/auditd.conf file and add or update the "name\_format" option:

```
name_format = hostname
```

The audit daemon must be restarted for changes to take effect.

#### **References:**

1. NIST SP 800-53 Revision 5 :: AU-4 (1)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230394  
Rule ID: SV-230394r877390  
STIG ID: RHEL-08-030062  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                              | IG 1 | IG 2 | IG 3 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.9 <u>Centralize Audit Logs</u></b><br>Centralize, to the extent possible, audit log collection and retention across enterprise assets.                          |      | ●    | ●    |
| v7               | <b>6.6 <u>Deploy SIEM or Log Analytic tool</u></b><br>Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis. |      | ●    | ●    |



### *6.3.1.8 Ensure the operating system's audit daemon is configured to resolve audit information before writing to disk (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must resolve audit information before writing to disk.

#### **Rationale:**

Without establishing what type of events occurred, the source of events, where events occurred, and the outcome of events, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Enriched logging aids in making sense of who, what, and when events occur on a system. Without this, determining root cause of an event will be much more difficult.

#### **Audit:**

Ensure the operating system's audit daemon is configured to resolve audit information before writing to disk, with the following command:

```
# grep "log_format" /etc/audit/auditd.conf  
  
log_format = ENRICHED
```

If the "log\_format" option is not "ENRICHED", or the line is commented out, this is a finding.

#### **Remediation:**

Edit the /etc/audit/auditd.conf file and add or update the "log\_format" option:

```
log_format = ENRICHED
```

The audit daemon must be restarted for changes to take effect.

#### **References:**

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230395  
Rule ID: SV-230395r627750  
STIG ID: RHEL-08-030063  
Severity: CAT III

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

### 6.3.2 Configure Data Retention

When auditing, it is important to carefully configure the storage requirements for audit logs. By default, auditd will max out the log files at 5MB and retain only 4 copies of them. Older versions will be deleted. It is possible on a system that the 20 MBs of audit logs may fill up the system causing loss of audit data. While the recommendations here provide guidance, check your site policy for audit storage requirements.

### 6.3.2.1 Ensure audit log storage size is configured (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

#### Description:

Configure the maximum size of the audit log file. Once the log reaches the maximum size, it will be rotated and a new log file will be started.

#### Rationale:

It is important that an appropriate size is determined for log files so that they do not impact the system and audit data is not lost.

#### Audit:

Run the following command and ensure output is in compliance with site policy:

```
# grep -Po -- '^h*max_log_fileh*=\h*\d+\b' /etc/audit/auditd.conf  
max_log_file = <MB>
```

#### Remediation:

Set the following parameter in `/etc/audit/auditd.conf` in accordance with site policy:

```
max_log_file = <MB>
```

#### Default Value:

```
max_log_file = 8
```

#### References:

1. NIST SP 800-53 Rev. 5: AU-8

#### Additional Information:

The `max_log_file` parameter is measured in megabytes.

Other methods of log rotation may be appropriate based on site policy. One example is time-based rotation strategies which don't have native support in `auditd` configurations. Manual audit of custom configurations should be evaluated for effectiveness and completeness.

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                  | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | 8.3 <u>Ensure Adequate Audit Log Storage</u><br>Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process. |  |  |  |
| v7               | 6.4 <u>Ensure adequate storage for logs</u><br>Ensure that all systems that store logs have adequate storage space for the logs generated.                               |                                                                                     |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0040  | M1053       |

### 6.3.2.2 Ensure audit logs are not automatically deleted (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

#### Description:

The `max_log_file_action` setting determines how to handle the audit log file reaching the max file size. A value of `keep_logs` will rotate the logs but never delete old logs.

#### Rationale:

In high security contexts, the benefits of maintaining a long audit history exceed the cost of storing the audit history.

#### Audit:

Run the following command and verify output matches:

```
# grep max_log_file_action /etc/audit/auditd.conf  
max_log_file_action = keep_logs
```

#### Remediation:

Set the following parameter in `/etc/audit/auditd.conf`:

```
max_log_file_action = keep_logs
```

#### Default Value:

`max_log_file_action = ROTATE`

#### References:

1. NIST SP 800-53 Rev. 5: AU-8

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                  | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | 8.3 <u>Ensure Adequate Audit Log Storage</u><br>Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process. | ●    | ●    | ●    |
| v7               | 6.4 <u>Ensure adequate storage for logs</u><br>Ensure that all systems that store logs have adequate storage space for the logs generated.                               |      | ●    | ●    |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0005  |             |

### 6.3.2.3 Ensure system is disabled when audit logs are full (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### Description:

The **auditd** daemon can be configured to halt the system or put the system in single user mode, if no free space is available or an error is detected on the partition that holds the audit log files.

The **disk\_full\_action** parameter tells the system what action to take when no free space is available on the partition that holds the audit log files. Valid values are **ignore**, **syslog**, **rotate**, **exec**, **suspend**, **single**, and **halt**.

- **ignore**, the audit daemon will issue a syslog message but no other action is taken
- **syslog**, the audit daemon will issue a warning to syslog
- **rotate**, the audit daemon will rotate logs, losing the oldest to free up space
- **exec**, /path-to-script will execute the script. You cannot pass parameters to the script. The script is also responsible for telling the auditd daemon to resume logging once its completed its action
- **suspend**, the audit daemon will stop writing records to the disk
- **single**, the audit daemon will put the computer system in single user mode
- **halt**, the audit daemon will shut down the system

The **disk\_error\_action** parameter tells the system what action to take when an error is detected on the partition that holds the audit log files. Valid values are **ignore**, **syslog**, **exec**, **suspend**, **single**, and **halt**.

- **ignore**, the audit daemon will not take any action
- **syslog**, the audit daemon will issue no more than 5 consecutive warnings to syslog
- **exec**, /path-to-script will execute the script. You cannot pass parameters to the script
- **suspend**, the audit daemon will stop writing records to the disk
- **single**, the audit daemon will put the computer system in single user mode
- **halt**, the audit daemon will shut down the system



## Rationale:

In high security contexts, the risk of detecting unauthorized access or nonrepudiation exceeds the benefit of the system's availability.

## Impact:

**disk\_full\_action** parameter:

- Set to **halt** - the **auditd** daemon will shutdown the system when the disk partition containing the audit logs becomes full.
- Set to **single** - the **auditd** daemon will put the computer system in single user mode when the disk partition containing the audit logs becomes full.

**disk\_error\_action** parameter:

- Set to **halt** - the **auditd** daemon will shutdown the system when an error is detected on the partition that holds the audit log files.
- Set to **single** - the **auditd** daemon will put the computer system in single user mode when an error is detected on the partition that holds the audit log files.
- Set to **syslog** - the **auditd** daemon will issue no more than 5 consecutive warnings to syslog when an error is detected on the partition that holds the audit log files.

## Audit:

Run the following command and verify the **disk\_full\_action** is set to either **halt** or **single**:

```
# grep -P -- '^h*disk_full_action\h*=\h*(halt|single)\b'
/etc/audit/auditd.conf

disk_full_action = <halt|single>
```

Run the following command and verify the **disk\_error\_action** is set to **syslog**, **single**, or **halt**:

```
# grep -P -- '^h*disk_error_action\h*=\h*(syslog|single|halt)\b'
/etc/audit/auditd.conf

disk_error_action = <syslog|single|halt>
```

## Remediation:

Set one of the following parameters in `/etc/audit/auditd.conf` depending on your local security policies.

```
disk_full_action = <halt|single>
disk_error_action = <syslog|single|halt>
```

### Example:

```
disk_full_action = halt
disk_error_action = halt
```

## References:

1. NIST SP 800-53 :: AU-5 b
2. NIST SP 800-53A :: AU-5.1 (iv)
3. AUDITD.CONF(5)
4. [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/8/html/security\\_hardening/auditing-the-system\\_security-hardening#configuring-auditd-for-a-secure-environment\\_auditing-the-system](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/auditing-the-system_security-hardening#configuring-auditd-for-a-secure-environment_auditing-the-system)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230390  
Rule ID: SV-230390r627750\_rule  
STIG ID: RHEL-08-030040  
Severity: CAT II

Vul ID: V-230392  
Rule ID: SV-230392r627750  
STIG ID: RHEL-08-030060  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                  | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.2 Collect Audit Logs</b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.  |  |  |  |
| v8               | <b>8.3 Ensure Adequate Audit Log Storage</b><br>Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process. |  |  |  |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1562, T1562.006                   | TA0005         |                    |

### 6.3.2.4 Ensure system warns when audit logs are low on space (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

#### Description:

The **auditd** daemon can be configured to halt the system, put the system in single user mode or send a warning message, if the partition that holds the audit log files is low on space.

The **space\_left\_action** parameter tells the system what action to take when the system has detected that it is starting to get low on disk space. Valid values are **ignore**, **syslog**, **rotate**, **email**, **exec**, **suspend**, **single**, and **halt**.

- **ignore**, the audit daemon does nothing
- **syslog**, the audit daemon will issue a warning to syslog
- **rotate**, the audit daemon will rotate logs, losing the oldest to free up space
- **email**, the audit daemon will send a warning to the email account specified in **action\_mail\_acct** as well as sending the message to syslog
- **exec**, /path-to-script will execute the script. You cannot pass parameters to the script. The script is also responsible for telling the auditd daemon to resume logging once its completed its action
- **suspend**, the audit daemon will stop writing records to the disk
- **single**, the audit daemon will put the computer system in single user mode
- **halt**, the audit daemon will shut down the system

The **admin\_space\_left\_action** parameter tells the system what action to take when the system has detected that it is low on disk space. Valid values are **ignore**, **syslog**, **rotate**, **email**, **exec**, **suspend**, **single**, and **halt**.

- **ignore**, the audit daemon does nothing
- **syslog**, the audit daemon will issue a warning to syslog
- **rotate**, the audit daemon will rotate logs, losing the oldest to free up space
- **email**, the audit daemon will send a warning to the email account specified in **action\_mail\_acct** as well as sending the message to syslog
- **exec**, /path-to-script will execute the script. You cannot pass parameters to the script. The script is also responsible for telling the auditd daemon to resume logging once its completed its action
- **suspend**, the audit daemon will stop writing records to the disk
- **single**, the audit daemon will put the computer system in single user mode
- **halt**, the audit daemon will shut down the system

## Rationale:

In high security contexts, the risk of detecting unauthorized access or nonrepudiation exceeds the benefit of the system's availability.

## Impact:

If the `admin_space_left_action` is set to `single` the audit daemon will put the computer system in single user mode.

## Audit:

Run the following command and verify the `space_left_action` is set to `email`, `exec`, `single`, or `halt`:

```
grep -P -- '^\h*space_left_action\h*=\h*(email|exec|single|halt)\b'
/etc/audit/auditd.conf
```

Verify the output is `email`, `exec`, `single`, or `halt`

*Example output*

```
space_left_action = email
```

Run the following command and verify the `admin_space_left_action` is set to `single` - OR - `halt`:

```
grep -P -- '^\h*admin_space_left_action\h*=\h*(single|halt)\b'
/etc/audit/auditd.conf
```

Verify the output is `single` or `halt`

*Example output:*

```
admin_space_left_action = single
```

**Note:** A Mail Transfer Agent (MTA) must be installed and configured properly to set `space_left_action = email`

## Remediation:

Set the `space_left_action` parameter in `/etc/audit/auditd.conf` to `email`, `exec`, `single`, or `halt`:

*Example:*

```
space_left_action = email
```

Set the `admin_space_left_action` parameter in `/etc/audit/auditd.conf` to `single` or `halt`:

*Example:*

```
admin_space_left_action = single
```

**Note:** A Mail Transfer Agent (MTA) must be installed and configured properly to set `space_left_action = email`

**Default Value:**

space\_left\_action = SYSLOG

admin\_space\_left\_action = SUSPEND

**References:**

1. NIST SP 800-53 Rev. 5: AU-2, AU-8, AU-12, SI-5
2. AUDITD.CONF(5)
3. [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/8/html/security\\_hardening/auditing-the-system\\_security-hardening#configuring-auditd-for-a-secure-environment\\_auditing-the-system](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/auditing-the-system_security-hardening#configuring-auditd-for-a-secure-environment_auditing-the-system)

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                  | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.2 Collect Audit Logs</b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.  |    |    |    |
| v8               | <b>8.3 Ensure Adequate Audit Log Storage</b><br>Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process. |  |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0005  |             |

### *6.3.2.5 Ensure the operating system allocates audit record storage capacity (Manual)*

**Profile Applicability:**

- STIG

**Description:**

The operating system must allocate audit record storage capacity to store at least one week of audit records, when audit records are not immediately sent to a central audit record storage facility.

**Rationale:**

To ensure the operating system has a sufficient storage capacity in which to write the audit logs, the operating system needs to be able to allocate audit record storage capacity.

The task of allocating audit record storage capacity is usually performed during initial installation of the operating system.

## Audit:

Verify the operating system allocates audit record storage capacity to store at least one week of audit records when audit records are not immediately sent to a central audit record storage facility.

Determine to which partition the audit records are being written with the following command:

```
# grep -iw log_file /etc/audit/auditd.conf  
  
log_file = /var/log/audit/audit.log
```

Check the size of the partition to which audit records are written (with the example being /var/log/audit/) with the following command:

```
# df -h /var/log/audit/  
  
/dev/sda2 24G 10.4G 13.6G 43% /var/log/audit
```

If the audit records are not written to a partition made specifically for audit records (/var/log/audit is a separate partition), determine the amount of space being used by other files in the partition with the following command:

```
# du -sh [audit_partition]  
  
1.8G /var/log/audit
```

If the audit record partition is not allocated for sufficient storage capacity, this is a finding.

Note: The partition size needed to capture a week of audit records is based on the activity level of the system and the total storage capacity available. Typically 10.0 GB of storage space for audit records should be sufficient.

## Remediation:

Allocate enough storage capacity for at least one week of audit records when audit records are not immediately sent to a central audit record storage facility.

If audit records are stored on a partition made specifically for audit records, resize the partition with sufficient space to contain one week of audit records.

If audit records are not stored on a partition made specifically for audit records, a new partition with sufficient space will need be to be created.

## References:

1. NIST SP 800-53 Revision 5 :: AU-4



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230476  
Rule ID: SV-230476r877391  
STIG ID: RHEL-08-030660  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                         | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.3 <u>Ensure Adequate Audit Log Storage</u></b><br>Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process. |  |  |  |
| v7               | <b>6.4 <u>Ensure adequate storage for logs</u></b><br>Ensure that all systems that store logs have adequate storage space for the logs generated.                               |                                                                                     |  |  |

### *6.3.2.6 Ensure the SA and ISSO are notified in the event of an audit processing failure (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) must be alerted of an audit processing failure event.

#### **Rationale:**

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

#### **Audit:**

Verify that the SA and ISSO (at a minimum) are notified in the event of an audit processing failure.

Check that the operating system notifies the SA and ISSO (at a minimum) in the event of an audit processing failure with the following command:

```
# grep action_mail_acct /etc/audit/auditd.conf  
  
action_mail_acct = root
```

If the value of the "action\_mail\_acct" keyword is not set to "root" and/or other accounts for security personnel, the "action\_mail\_acct" keyword is missing, or the retuned line is commented out, ask the system administrator to indicate how they and the ISSO are notified of an audit process failure. If there is no evidence of the proper personnel being notified of an audit processing failure, this is a finding.

**Remediation:**

Configure "auditd" service to notify the SA and ISSO in the event of an audit processing failure.  
Edit the following line in "/etc/audit/auditd.conf" to ensure that administrators are notified via email for those situations:

```
action_mail_acct = root
```

**References:**

- 1. NIST SP 800-53 Revision 5 :: AU-5 a
- 2. NIST SP 800-53A :: AU-5.1 (ii)

**Additional Information:**

Red Hat Enterprise Linux 8 Security Technical Implementation Guide

Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230388

Rule ID: SV-230388r627750

STIG ID: RHEL-08-030020

Severity: CAT II

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                 | IG 1        | IG 2        | IG 3        |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-------------|-------------|
| v8               | 8.2 <u>Collect Audit Logs</u><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. | <div></div> | <div></div> | <div></div> |
| v7               | 6.2 <u>Activate audit logging</u><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  | <div></div> | <div></div> | <div></div> |

### *6.3.2.7 Ensure the operating system notifies the SA and ISSO when allocated audit record storage volume reaches 75 percent (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) when allocated audit record storage volume 75 percent utilization.

#### **Rationale:**

If security personnel are not notified immediately when storage volume reaches 75 percent utilization, they are unable to plan for audit record storage capacity expansion.

#### **Audit:**

Verify the operating system notifies the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity with the following command:

```
# grep -w space_left_action /etc/audit/auditd.conf  
  
space_left_action = email
```

If the value of the "space\_left\_action" is not set to "email", or if the line is commented out, ask the System Administrator to indicate how the system is providing real-time alerts to the SA and ISSO.

If there is no evidence that real-time alerts are configured on the system, this is a finding.

#### **Remediation:**

Configure the operating system to initiate an action to notify the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity by adding/modifying the following line in the "/etc/audit/auditd.conf" file.

```
space_left_action = email
```

Note: Option names and values in the auditd.conf file are case insensitive.

#### **References:**

1. NIST SP 800-53 Revision 5 :: AU-5 (1)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244543  
Rule ID: SV-244543r877389  
STIG ID: RHEL-08-030731  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                         | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.3 <u>Ensure Adequate Audit Log Storage</u></b><br>Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process. |  |  |  |
| v7               | <b>6.4 <u>Ensure adequate storage for logs</u></b><br>Ensure that all systems that store logs have adequate storage space for the logs generated.                               |                                                                                     |  |  |

### *6.3.2.8 Ensure the operating system takes action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must take action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity.

#### **Rationale:**

If security personnel are not notified immediately when storage volume reaches 75 percent utilization, they are unable to plan for audit record storage capacity expansion.

#### **Audit:**

Verify the operating system takes action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity with the following commands:

```
# grep -w space_left /etc/audit/auditd.conf  
  
space_left = 25%
```

If the value of the "space\_left" keyword is not set to "25%" or if the line is commented out, ask the System Administrator to indicate how the system is providing real-time alerts to the SA and ISSO.

If there is no evidence that real-time alerts are configured on the system, this is a finding.

#### **Remediation:**

Configure the operating system to initiate an action to notify the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity by adding/modifying the following line in the /etc/audit/auditd.conf file.

```
space_left = 25%
```

Note: Option names and values in the auditd.conf file are case insensitive.

#### **References:**

1. NIST SP 800-53 Revision 5 :: AU-5 (1)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230483  
Rule ID: SV-230483r877389  
STIG ID: RHEL-08-030730  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                         | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.3 <u>Ensure Adequate Audit Log Storage</u></b><br>Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process. |  |  |  |
| v7               | <b>6.4 <u>Ensure adequate storage for logs</u></b><br>Ensure that all systems that store logs have adequate storage space for the logs generated.                               |                                                                                     |  |  |

### *6.3.2.9 Ensure the audit system is configured to take an appropriate action when the internal event queue is full (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must take appropriate action when the internal event queue is full.

#### **Rationale:**

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

The operating system's installation media provides "rsyslogd". "rsyslogd" is a system utility providing support for message logging. Support for both internet and UNIX domain sockets enables this utility to support both local and remote logging. Couple this utility with "gnutls" (which is a secure communications library implementing the SSL, TLS and DTLS protocols), and you have a method to securely encrypt and off-load auditing.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

#### **Audit:**

Verify the audit system is configured to take an appropriate action when the internal event queue is full:

```
# grep -i overflow_action /etc/audit/auditd.conf  
  
overflow_action = syslog
```

If the value of the "overflow\_action" option is not set to "syslog", "single", "halt", or the line is commented out, ask the System Administrator to indicate how the audit logs are off-loaded to a different system or media.

If there is no evidence that the transfer of the audit logs being off-loaded to another system or media takes appropriate action if the internal event queue becomes full, this is a finding.



## Remediation:

Edit the `/etc/audit/auditd.conf` file and add or update the "overflow\_action" option:

```
overflow_action = syslog
```

The audit daemon must be restarted for changes to take effect.

## References:

1. NIST SP 800-53 Revision 5 :: AU-4 (1)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230480  
Rule ID: SV-230480r877390  
STIG ID: RHEL-08-030700  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                         | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.3 <u>Ensure Adequate Audit Log Storage</u></b><br>Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process. |  |  |  |
| v7               | <b>6.4 <u>Ensure adequate storage for logs</u></b><br>Ensure that all systems that store logs have adequate storage space for the logs generated.                               |                                                                                       |  |  |

### 6.3.3 Configure auditd Rules

The Audit system operates on a set of rules that define what is to be captured in the log files.

The following types of Audit rules can be specified:

- Control rules: Allow the Audit system's behavior and some of its configuration to be modified.
- File system rules: Allow the auditing of access to a particular file or a directory. (Also known as file watches)
- System call rules: Allow logging of system calls that any specified program makes.

Audit rules can be set:

- on the command line using the `auditctl` utility. Note that these rules are not persistent across reboots.
- in a file ending in `.rules` in the `/etc/audit/rules.d/` directory.

### *6.3.3.1 Ensure changes to system administration scope (sudoers) is collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### **Description:**

Monitor scope changes for system administrators. If the system has been properly configured to force system administrators to log in as themselves first and then use the **sudo** command to execute privileged commands, it is possible to monitor changes in scope. The file **/etc/sudoers**, or files in **/etc/sudoers.d**, will be written to when the file(s) or related attributes have changed. The audit records will be tagged with the identifier "scope".

#### **Rationale:**

Changes in the **/etc/sudoers** and **/etc/sudoers.d** files can indicate that an unauthorized change has been made to the scope of system administrator activity.

## Audit:

### On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&/\etc\sudoers/ \
&&/ +-p *wa/ \
&&( / key= *[-~]* *$||/ -k *[-~]* *$/) ' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d -p wa -k scope
```

### Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&/\etc\sudoers/ \
&&/ +-p *wa/ \
&&( / key= *[-~]* *$||/ -k *[-~]* *$/) '
```

Verify the output matches:

```
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d -p wa -k scope
```

## Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor scope changes for system administrators.

*Example:*

```
# printf '%s\n' "-w /etc/sudoers -p wa -k scope" "-w /etc/sudoers.d -p wa -k scope" >> /etc/audit/rules.d/50-scope.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230409  
Rule ID: SV-230409r627750\_rule  
STIG ID: RHEL-08-030171  
Severity: CAT II

Vul ID: V-230410  
Rule ID: SV-230410r627750  
STIG ID: RHEL-08-030172  
Severity: CAT II

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000304-GPOS-00121, CCI-002884, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221

Potential reboot required

If the auditing configuration is locked (**-e 2**), then **augenrules** will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

System call structure

For performance (**man 7 audit.rules**) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | 8.5 <u>Collect Detailed Audit Logs</u><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      |      |      |
| v7               | 4.8 <u>Log and Alert on Changes to Administrative Group Membership</u><br>Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.                                                                           |      |      |      |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1562, T1562.006                   | TA0004         | M1047              |

### *6.3.3.2 Ensure actions as another user are always logged (Automated)*

**Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation
- STIG

**Description:**

`sudo` provides users with temporary elevated privileges to perform operations, either as the superuser or another user.

**Rationale:**

Creating an audit log of users with temporary elevated privileges and the operation(s) they performed is essential to reporting. Administrators will want to correlate the events written to the audit trail with the records written to `sudo`'s logfile to verify if unauthorized commands have been executed.

## Audit:

### On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-a *always,exit/ \
&&/ -F *arch=b(32|64)/ \
&&/ -F *audit!=unset/||/ -F *audit!=-1/||/ -F *audit!=4294967295/) \
&&/ -C *euid!=uid/||/ -C *uid!=euid/) \
&&/ -S *execve/ \
&&/ key= *![!~]* *$/||/ -k *![!~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-a always,exit -F arch=b64 -C euid!=uid -F audit!=unset -S execve -k
user_emulation
-a always,exit -F arch=b32 -C euid!=uid -F audit!=unset -S execve -k
user_emulation
```

### Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-a *always,exit/ \
&&/ -F *arch=b(32|64)/ \
&&/ -F *audit!=unset/||/ -F *audit!=-1/||/ -F *audit!=4294967295/) \
&&/ -C *euid!=uid/||/ -C *uid!=euid/) \
&&/ -S *execve/ \
&&/ key= *![!~]* *$/||/ -k *![!~]* *$/)'
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S execve -C uid!=euid -F audit!=-1 -F
key=user_emulation
-a always,exit -F arch=b32 -S execve -C uid!=euid -F audit!=-1 -F
key=user_emulation
```



## Remediation:

### Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor elevated privileges.

*Example:*

```
# printf "  
-a always,exit -F arch=b64 -C euid!=uid -F auid!=unset -S execve -k  
user_emulation  
-a always,exit -F arch=b32 -C euid!=uid -F auid!=unset -S execve -k  
user_emulation  
" >> /etc/audit/rules.d/50-user_emulation.rules
```

### Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot  
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 Revision 5 :: AC-6 (8)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230386  
Rule ID: SV-230386r854037  
STIG ID: RHEL-08-030000  
Severity: CAT II

Satisfies: SRG-OS-000326-GPOS-00126, SRG-OS-000327-GPOS-00127

### Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      |  |  |
| v7               | <b>4.9 <u>Log and Alert on Unsuccessful Administrative Account Login</u></b><br>Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.                                                                                                                 |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0004  | M1047       |

### *6.3.3.3 Ensure events that modify the sudo log file are collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

Monitor the `sudo` log file. If the system has been properly configured to disable the use of the `su` command and force all administrators to have to log in first and then use `sudo` to execute privileged commands, then all administrator commands will be logged to `/var/log/sudo.log`. Any time a command is executed, an audit event will be triggered as the `/var/log/sudo.log` file will be opened for write and the executed administration command will be written to the log.

#### **Rationale:**

Changes in `/var/log/sudo.log` indicate that an administrator has executed a command or the log file itself has been tampered with. Administrators will want to correlate the events written to the audit trail with the records written to `/var/log/sudo.log` to verify if unauthorized commands have been executed.

## Audit:

**Note:** This recommendation requires that the sudo logfile is configured. See guidance provided in the recommendation "Ensure sudo log file exists"

### On disk configuration

Run the following command to check the on disk rules:

```
# {
  SUDO_LOG_FILE=$(grep -r logfile /etc/sudoers* | sed -e 's/.*logfile=//;s/,?
.*//'-e 's"/"/g' -e 's|/|\\|/g')
  [ -n "${SUDO_LOG_FILE}" ] && awk "/^ *-w/ \
&&/${SUDO_LOG_FILE}"/ \
&&/ +-p *wa/ \
&&( / key= *[-~]* *$/||/ -k *[-~]* *$/)" /etc/audit/rules.d/*.rules \
|| printf "ERROR: Variable 'SUDO_LOG_FILE' is unset.\n"
}
```

Verify output of matches:

```
-w /var/log/sudo.log -p wa -k sudo_log_file
```

### Running configuration

Run the following command to check loaded rules:

```
# {
  SUDO_LOG_FILE=$(grep -r logfile /etc/sudoers* | sed -e 's/.*logfile=//;s/,?
.*//'-e 's"/"/g' -e 's|/|\\|/g')
  [ -n "${SUDO_LOG_FILE}" ] && auditctl -l | awk "/^ *-w/ \
&&/${SUDO_LOG_FILE}"/ \
&&/ +-p *wa/ \
&&( / key= *[-~]* *$/||/ -k *[-~]* *$/)" \
|| printf "ERROR: Variable 'SUDO_LOG_FILE' is unset.\n"
}
```

Verify output matches:

```
-w /var/log/sudo.log -p wa -k sudo_log_file
```

## Remediation:

**Note:** This recommendation requires that the sudo logfile is configured. See guidance provided in the recommendation "Ensure sudo log file exists"

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify the sudo log file.

*Example:*

```
# {
SUDO_LOG_FILE=$(grep -r logfile /etc/sudoers* | sed -e 's/.*/logfile=//;s/,?
.*//' -e 's/"//g')
[ -n "${SUDO_LOG_FILE}" ] && printf "
-w ${SUDO_LOG_FILE} -p wa -k sudo_log_file
" >> /etc/audit/rules.d/50-sudo.rules || printf "ERROR: Variable
'SUDO_LOG_FILE' is unset.\n"
}
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## Additional Information:

### Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      |  |  |
| v7               | <b>4.9 <u>Log and Alert on Unsuccessful Administrative Account Login</u></b><br>Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.                                                                                                                 |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0004  |             |

### 6.3.3.4 Ensure events that modify date and time information are collected (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

#### Description:

Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the;

- **adjtimex** - tune kernel clock
- **settimeofday** - set time using **timeval** and **timezone** structures
- **stime** - using seconds since 1/1/1970
- **clock\_settime** - allows for the setting of several internal clocks and timers

system calls have been executed. Further, ensure to write an audit record to the configured audit log file upon exit, tagging the records with a unique identifier such as "time-change".

#### Rationale:

Unexpected changes in system date and/or time could be a sign of malicious activity on the system.

#### Audit:

##### On disk configuration

Run the following command to check the on disk rules:

```
# {
awk '/^ *-a *always,exit/ \
&&/ -F *arch=b(32|64)/ \
&&/ -S/ \
&&(/adjtimex/ \
||/settimeofday/ \
||/clock_settime/ ) \
&&(/ key= *[-~]* *$/||/ -k *[-~]* *$/)' /etc/audit/rules.d/*.rules

awk '/^ *-w/ \
&&/\etc\localtime/ \
&&/ +-p *wa/ \
&&(/ key= *[-~]* *$/||/ -k *[-~]* *$/)' /etc/audit/rules.d/*.rules
}
```

Verify output of matches:

```
-a always,exit -F arch=b64 -S adjtimex,settimeofday -k time-change
-a always,exit -F arch=b32 -S adjtimex,settimeofday -k time-change
-a always,exit -F arch=b64 -S clock_settime -F a0=0x0 -k time-change
-a always,exit -F arch=b32 -S clock_settime -F a0=0x0 -k time-change
-w /etc/localtime -p wa -k time-change
```

## Running configuration

Run the following command to check loaded rules:

```
# {
  auditctl -l | awk '/^ *-a *always,exit/ \
    &&/ -F *arch=b(32|64)/ \
    &&/ -S/ \
    &&(/adjtimex/ \
      ||/settimeofday/ \
      ||/clock_settime/ ) \
    &&(/ key= *[:-~]* *$/||/ -k *[:-~]* *$/)'

  auditctl -l | awk '/^ *-w/ \
    &&/\etc\localtime/ \
    &&/ +-p *wa/ \
    &&(/ key= *[:-~]* *$/||/ -k *[:-~]* *$/)'
}
```

Verify the output includes:

```
-a always,exit -F arch=b64 -S adjtimex,settimeofday -F key=time-change
-a always,exit -F arch=b32 -S settimeofday,adjtimex -F key=time-change
-a always,exit -F arch=b64 -S clock_settime -F a0=0x0 -F key=time-change
-a always,exit -F arch=b32 -S clock_settime -F a0=0x0 -F key=time-change
-w /etc/localtime -p wa -k time-change
```



## Remediation:

### Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify date and time information.

Example:

```
# printf "  
-a always,exit -F arch=b64 -S adjtimex,settimeofday -k time-change  
-a always,exit -F arch=b32 -S adjtimex,settimeofday -k time-change  
-a always,exit -F arch=b64 -S clock_settime -F a0=0x0 -k time-change  
-a always,exit -F arch=b32 -S clock_settime -F a0=0x0 -k time-change  
-w /etc/localtime -p wa -k time-change  
" >> /etc/audit/rules.d/50-time-change.rules
```

### Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot  
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3, CM-6

## Additional Information:

### Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### System call structure

For performance ([man 7 audit.rules](#)) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      |  |  |
| v7               | <b>5.5 <u>Implement Automated Configuration Monitoring Systems</u></b><br>Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.      |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0005  | M1047       |

### 6.3.3.5 Ensure events that modify the system's network environment are collected (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

#### Description:

Record changes to network environment files or system calls. The below parameters monitors the following system calls, and write an audit event on system call exit:

- `sethostname` - set the systems host name
- `setdomainname` - set the systems domain name

The files being monitored are:

- `/etc/issue` and `/etc/issue.net` - messages displayed pre-login
- `/etc/hosts` - file containing host names and associated IP addresses
- `/etc/hostname` - file contains the system's host name
- `/etc/sysconfig/network` - additional information that is valid to all network interfaces
- `/etc/sysconfig/network-scripts/` - directory containing network interface scripts and configurations files
- `/etc/NetworkManager/` - directory contains configuration files and settings used by the `NetworkManager`

#### Rationale:

Monitoring `sethostname` and `setdomainname` will identify potential unauthorized changes to host and domain name of a system. The changing of these names could potentially break security parameters that are set based on those names. The `/etc/hosts` file is monitored for changes that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring `/etc/issue` and `/etc/issue.net` is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring `/etc/sysconfig/network` is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised. All audit records should have a relevant tag associated with them.

## Audit:

### On disk configuration

Run the following commands to check the on disk rules:

```
# {
# Check for syscalls related to hostname and domainname change
awk '/^*-a *always, exit/ \
&& /-F *arch=b(32|64)/ \
&& /-S/ && (/sethostname/ \
|| /setdomainname/) \
&& (/key= *[:-~]* *$/ || /-k *[:-~]* *$/)' /etc/audit/rules.d/*.rules

# Check for file watches on network-related files
awk '/^ *-w/ \
&& (/etc\issue/ \
|| /etc\issue.net/ \
|| /etc\hosts/ \
|| /etc\sysconfig\network/ \
|| /etc\hostname/ \
|| /etc\NetworkManager/) \
&& / +-p *wa/ \
&& (/ key= *[:-~]* *$/ || /-k *[:-~]* *$/)' /etc/audit/rules.d/*.rules
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S sethostname,setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname,setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/hostname -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
-w /etc/sysconfig/network-scripts/ -p wa -k system-locale
-w /etc/NetworkManager -p wa -k system-locale
```

### Running configuration

Run the following command to check loaded rules:

```
# {
auditctl -l | awk '/^ *-a *always,exit/ \
&&/ -F *arch=b(32|64)/ \
&&/ -S/ \
&&(/sethostname/ \
||/setdomainname/) \
&&(/ key= *[:-~]* *$/||/ -k *[:-~]* *$/)'

auditctl -l | awk '/^ *-w/ \
&&/etc\/issue/ \
|| /etc\/issue.net/ \
|| /etc\/hosts/ \
|| /etc\/sysconfig\/network/ \
|| /etc\/hostname/ \
|| /etc\/NetworkManager/) \
&&/ +-p *wa/ \
&&(/ key= *[:-~]* *$/||/ -k *[:-~]* *$/)'
}
```

Verify the output includes:

```
-a always,exit -F arch=b64 -S sethostname,setdomainname -F key=system-locale
-a always,exit -F arch=b32 -S sethostname,setdomainname -F key=system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/hostname -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
-w /etc/sysconfig/network-scripts -p wa -k system-locale
-w /etc/NetworkManager -p wa -k system-locale
```

## Remediation:

### Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify the system's network environment.

Example:

```
# printf "  
-a always,exit -F arch=b64 -S sethostname,setdomainname -k system-locale  
-a always,exit -F arch=b32 -S sethostname,setdomainname -k system-locale  
-w /etc/issue -p wa -k system-locale  
-w /etc/issue.net -p wa -k system-locale  
-w /etc/hosts -p wa -k system-locale  
-w /etc/hostname -p wa -k system-locale  
-w /etc/sysconfig/network -p wa -k system-locale  
-w /etc/sysconfig/network-scripts/ -p wa -k system-locale  
-w /etc/NetworkManager -p wa -k system-locale  
" >> /etc/audit/rules.d/50-system_locale.rules
```

### Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot  
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3, CM-6

## Additional Information:

### Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### System call structure

For performance ([man 7 audit.rules](#)) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      |  |  |
| v7               | <b>5.5 <u>Implement Automated Configuration Monitoring Systems</u></b><br>Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.      |      |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0003  | M1047       |

### 6.3.3.6 *Ensure use of privileged commands are collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

Monitor privileged programs, those that have the **setuid** and/or **setgid** bit set on execution, to determine if unprivileged users are running these commands.

#### **Rationale:**

Execution of privileged commands by non-privileged users could be an indication of someone trying to gain unauthorized access to the system.

#### **Impact:**

Both the audit and remediation section of this recommendation will traverse all mounted file systems that is not mounted with either **noexec** or **nosuid** mount options. If there are large file systems without these mount options, **such traversal will be significantly detrimental to the performance of the system.**

Before running either the audit or remediation section, inspect the output of the following command to determine exactly which file systems will be traversed:

```
# findmnt -n -l -k -it $(awk '/nodev/ { print $2 }' /proc/filesystems | paste -sd,) | grep -Pv "noexec|nosuid"
```

To exclude a particular file system due to adverse performance impacts, update the audit and remediation sections by adding a sufficiently unique string to the **grep** statement. The above command can be used to test the modified exclusions.



## Audit:

### On disk configuration

Run the following script to check on disk rules:

```
#!/usr/bin/env bash

{
    for PARTITION in $(findmnt -n -l -k -it $(awk '/nodev/ { print $2 }'
/proc/filesystems | paste -sd,) | grep -Pv "noexec|nosuid" | awk '{print
$1}'); do
        for PRIVILEGED in $(find "${PARTITION}" -xdev -perm /6000 -type f); do
            grep -qr "${PRIVILEGED}" /etc/audit/rules.d && printf "OK:
'${PRIVILEGED}' found in auditing rules.\n" || printf "Warning:
'${PRIVILEGED}' not found in on disk configuration.\n"
        done
    done
}
```

Verify that all output is **OK**.

### Running configuration

Run the following script to check loaded rules:

```
#!/usr/bin/env bash

{
    RUNNING=$(auditctl -l)
    [ -n "${RUNNING}" ] && for PARTITION in $(findmnt -n -l -k -it $(awk
'/nodev/ { print $2 }' /proc/filesystems | paste -sd,) | grep -Pv
"noexec|nosuid" | awk '{print $1}'); do
        for PRIVILEGED in $(find "${PARTITION}" -xdev -perm /6000 -type f); do
            printf -- "${RUNNING}" | grep -q "${PRIVILEGED}" && printf "OK:
'${PRIVILEGED}' found in auditing rules.\n" || printf "Warning:
'${PRIVILEGED}' not found in running configuration.\n"
        done
    done \
    || printf "ERROR: Variable 'RUNNING' is unset.\n"
}
```

Verify that all output is **OK**.

### Special mount points

If there are any special mount points that are not visible by default from **findmnt** as per the above audit, said file systems would have to be manually audited.

## Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor the use of privileged commands.

*Example script:*

```
#!/usr/bin/env bash

{
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  AUDIT_RULE_FILE="/etc/audit/rules.d/50-privileged.rules"
  NEW_DATA=()
  for PARTITION in $(findmnt -n -l -k -it $(awk '/nodev/ { print $2 }' /proc/filesystems | paste -sd,) | grep -Pv "noexec|nosuid" | awk '{print $1}'); do
    readarray -t DATA <<(find "${PARTITION}" -xdev -perm /6000 -type f | awk -v UID_MIN=${UID_MIN} '{print "-a always,exit -F path=" $1 " -F perm=x -F auid>="UID_MIN" -F auid!=unset -k privileged" }')
    for ENTRY in "${DATA[@]}"; do
      NEW_DATA+=("${ENTRY}")
    done
  done
  readarray &> /dev/null -t OLD_DATA < "${AUDIT_RULE_FILE}"
  COMBINED_DATA=( "${OLD_DATA[@]}" "${NEW_DATA[@]}" )
  printf '%s\n' "${COMBINED_DATA[@]}" | sort -u > "${AUDIT_RULE_FILE}"
}
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot required to load rules\n"; fi
```

## Special mount points

If there are any special mount points that are not visible by default from just scanning `/`, change the `PARTITION` variable to the appropriate partition and re-run the remediation.

## References:

1. NIST SP 800-53 Rev. 5: AU-3, AU-3(1)

## Additional Information:

### Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |                                                                                       |    |    |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         |  |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0002  | M1026       |

### *6.3.3.7 Ensure unsuccessful file access attempts are collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### **Description:**

Monitor for unsuccessful attempts to access files. The following parameters are associated with system calls that control files:

- creation - **creat**
- opening - **open** , **openat**
- truncation - **truncate** , **ftruncate**

An audit log record will only be written if all of the following criteria is met for the user when trying to access a file:

- a non-privileged user (auid>=UID\_MIN)
- is not a Daemon event (auid=4294967295/unset/-1)
- if the system call returned EACCES (permission denied) or EPERM (some other permanent error associated with the specific system call)

#### **Rationale:**

Failed attempts to open, create or truncate files could be an indication that an individual or process is trying to gain unauthorized access to the system.

## Audit:

### On disk configuration

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
&&/ -F *arch=b(32|64)/ \
&&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&(/ -F *exit==EACCES/||/ -F *exit==EPERM/) \
&&/ -S/ \
&&/creat/ \
&&/open/ \
&&/truncate/ \
&&(/ key= *[-~]* *$/||/ -k *[-~]* *$/)" /etc/audit/rules.d/*.rules \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output includes:

```
-a always,exit -F arch=b64 -S creat,open,openat,truncate,ftruncate -F exit==
EACCES -F auid>=1000 -F auid!=unset -k access
-a always,exit -F arch=b64 -S creat,open,openat,truncate,ftruncate -F exit==
EPERM -F auid>=1000 -F auid!=unset -k access
-a always,exit -F arch=b32 -S creat,open,openat,truncate,ftruncate -F exit==
EACCES -F auid>=1000 -F auid!=unset -k access
-a always,exit -F arch=b32 -S creat,open,openat,truncate,ftruncate -F exit==
EPERM -F auid>=1000 -F auid!=unset -k access
```

### Running configuration

Run the following command to check loaded rules:

```
# {
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
&&/ -F *arch=b(32|64)/ \
&&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&(/ -F *exit==EACCES/||/ -F *exit==EPERM/) \
&&/ -S/ \
&&/creat/ \
&&/open/ \
&&/truncate/ \
&&(/ key= *[-~]* *$/||/ -k *[-~]* *$/)" \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output includes:

```
-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat -F exit=-EACCES -F auid>=1000 -F auid!=-1 -F key=access
-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat -F exit=-EPERM -F auid>=1000 -F auid!=-1 -F key=access
-a always,exit -F arch=b32 -S open,truncate,ftruncate,creat,openat -F exit=-EACCES -F auid>=1000 -F auid!=-1 -F key=access
-a always,exit -F arch=b32 -S open,truncate,ftruncate,creat,openat -F exit=-EPERM -F auid>=1000 -F auid!=-1 -F key=access
```

## Remediation:

### Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor unsuccessful file access attempts.

*Example:*

```
# {
UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b64 -S creat,open,openat,truncate,ftruncate -F exit=-EACCES -F auid>=${UID_MIN} -F auid!=unset -k access
-a always,exit -F arch=b64 -S creat,open,openat,truncate,ftruncate -F exit=-EPERM -F auid>=${UID_MIN} -F auid!=unset -k access
-a always,exit -F arch=b32 -S creat,open,openat,truncate,ftruncate -F exit=-EACCES -F auid>=${UID_MIN} -F auid!=unset -k access
-a always,exit -F arch=b32 -S creat,open,openat,truncate,ftruncate -F exit=-EPERM -F auid>=${UID_MIN} -F auid!=unset -k access
" >> /etc/audit/rules.d/50-access.rules || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

### Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230449  
Rule ID: SV-230449r810455  
STIG ID: RHEL-08-030420  
Severity: CAT II

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000064-GPOS-00033

## Potential reboot required

If the auditing configuration is locked (**-e 2**), then **augenrules** will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

## System call structure

For performance (**man 7 audit.rules**) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      |  |  |
| v7               | <b>14.9 Enforce Detail Logging for Access or Changes to Sensitive Data</b><br>Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).                       |      |                                                                                       |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0007  |             |

### 6.3.3.8 Ensure events that modify user/group information are collected (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### Description:

Record events affecting the modification of user or group information, including that of passwords and old passwords if in use.

- `/etc/group` - system groups
- `/etc/passwd` - system users
- `/etc/gshadow` - encrypted password for each group
- `/etc/shadow` - system user passwords
- `/etc/security/opasswd` - storage of old passwords if the relevant PAM module is in use
- `/etc/nsswitch.conf` - file configures how the system uses various databases and name resolution mechanisms
- `/etc/pam.conf` - file determines the authentication services to be used, and the order in which the services are used.
- `/etc/pam.d` - directory contains the PAM configuration files for each PAM-aware application.

The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier "identity" in the audit log file.

#### Rationale:

Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.



## Audit:

### On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&(/\/etc\/group/ \
  ||\/etc\/passwd/ \
  ||\/etc\/gshadow/ \
  ||\/etc\/shadow/ \
  ||\/etc\/security\/opasswd/ \
  ||\/etc\/nsswitch.conf/ \
  ||\/etc\/pam.conf/ \
  ||\/etc\/pam.d/) \
&&/ +-p *wa/ \
&&(/ key= *![!~]* *$/||/ -k *![!~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
-w /etc/nsswitch.conf -p wa -k identity
-w /etc/pam.conf -p wa -k identity
-w /etc/pam.d -p wa -k identity
```

### Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&(/\/etc\/group/ \
  ||\/etc\/passwd/ \
  ||\/etc\/gshadow/ \
  ||\/etc\/shadow/ \
  ||\/etc\/security\/opasswd/ \
  ||\/etc\/nsswitch.conf/ \
  ||\/etc\/pam.conf/ \
  ||\/etc\/pam.d/) \
&&/ +-p *wa/ \
&&(/ key= *![!~]* *$/||/ -k *![!~]* *$/)'
```

Verify the output matches:

```
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
-w /etc/nsswitch.conf -p wa -k identity
-w /etc/pam.conf -p wa -k identity
-w /etc/pam.d -p wa -k identity
```

## Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify user/group information.

*Example:*

```
# printf "
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
-w /etc/nsswitch.conf -p wa -k identity
-w /etc/pam.conf -p wa -k identity
-w /etc/pam.d -p wa -k identity
" >> /etc/audit/rules.d/50-identity.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)
3. <https://manpages.debian.org/bookworm/manpages/nsswitch.conf.5.en.html>
4. [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/6/html/managing\\_smart\\_cards/pam\\_configuration\\_files](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/managing_smart_cards/pam_configuration_files)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230404  
Rule ID: SV-230404r627750  
STIG ID: RHEL-08-030130  
Severity: CAT II

Vul ID: V-230405  
Rule ID: SV-230405r627750  
STIG ID: RHEL-08-030140  
Severity: CAT II

Vul ID: V-230406  
Rule ID: SV-230406r627750  
STIG ID: RHEL-08-030150  
Severity: CAT II

Vul ID: V-230407  
Rule ID: SV-230407r627750  
STIG ID: RHEL-08-030160  
Severity: CAT II

Vul ID: V-230408  
Rule ID: SV-230408r627750  
STIG ID: RHEL-08-030170  
Severity: CAT II

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000304-GPOS-00121, SRG-OS-000476-GPOS-00221

### Potential reboot required

If the auditing configuration is locked (**-e 2**), then **augenrules** will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### System call structure

For performance (**man 7 audit.rules**) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      |  |  |
| v7               | <b>4.8 <u>Log and Alert on Changes to Administrative Group Membership</u></b><br>Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.                                                                           |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0004  | M1047       |

### *6.3.3.9 Ensure discretionary access control permission modification events are collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### **Description:**

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The following commands and system calls effect the permissions, ownership and various attributes of files.

- `chmod`
- `fchmod`
- `fchmodat`
- `chown`
- `fchown`
- `fchownat`
- `lchown`
- `setxattr`
- `lsetxattr`
- `fsetxattr`
- `removexattr`
- `lremovexattr`
- `fremovexattr`

In all cases, an audit record will only be written for non-system user ids and will ignore Daemon events. All audit records will be tagged with the identifier "perm\_mod."

#### **Rationale:**

Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

## Audit:

**Note:** Output showing all audited syscalls, e.g. (-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat,chmod,fchmod,fchmodat,setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F auid>=1000 -F auid!=unset -F key=perm\_mod) is also acceptable. These have been separated by function on the displayed output for clarity.

### On disk configuration

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
&&/ -F *arch=b(32|64)/ \
&&/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -S/ \
&&/ -F *auid>=${UID_MIN}/ \
&&(/chmod/||/fchmod/||/fchmodat/ \
  ||/chown/||/fchown/||/fchownat/||/lchown/ \
  ||/setxattr/||/lsetxattr/||/fsetxattr/ \
  ||/removexattr/||/lremovexattr/||/fremovexattr/) \
&&(/ key= *[^~]* *$/||/ -k *[^~]* *$/)" /etc/audit/rules.d/*.rules \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S chown,fchown,lchown,fchownat -F auid>=1000 -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F auid>=1000 -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid!=unset -F key=perm_mod
```

### Running configuration

Run the following command to check loaded rules:

```
# {
UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
&&/ -F *arch=b(32|64)/ \
&&/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -S/ \
&&/ -F *auid>=${UID_MIN}/ \
&&(/chmod/||/fchmod/||/fchmodat/ \
||/chown/||/fchown/||/fchownat/||/lchown/ \
||/setxattr/||/lsetxattr/||/fsetxattr/ \
||/removexattr/||/lremovexattr/||/fremovexattr/) \
&&(/ key= *[:-~]* *$/||/ -k *[:-~]* *$/)" \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1
-F key=perm_mod
-a always,exit -F arch=b64 -S chown,fchown,lchown,fchownat -F auid>=1000 -F
auid!=-1 -F key=perm_mod
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1
-F key=perm_mod
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F auid>=1000 -F
auid!=-1 -F key=perm_mod
-a always,exit -F arch=b64 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b32 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid!=-1 -F key=perm_mod
```

## Remediation:

### Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor discretionary access control permission modification events.

*Example:*

```
# {
UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=${UID_MIN} -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S chown,fchown,lchown,fchownat -F
auid>=${UID_MIN} -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=${UID_MIN} -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F
auid>=${UID_MIN} -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=${UID_MIN} -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=${UID_MIN} -F auid!=unset -F key=perm_mod
" >> /etc/audit/rules.d/50-perm_mod.rules || printf "ERROR: Variable
'UID_MIN' is unset.\n"
}
```

### Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230413  
Rule ID: SV-230413r810463  
STIG ID: RHEL-08-030200  
Severity: CAT II

Vul ID: V-230455  
Rule ID: SV-230455r810459  
STIG ID: RHEL-08-030480  
Severity: CAT II

Vul ID: V-230456  
Rule ID: SV-230456r810462  
STIG ID: RHEL-08-030490  
Severity: CAT II

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000064-GPOS-00033, SRG-OS-000466-GPOS-00210

## Potential reboot required

If the auditing configuration is locked (**-e 2**), then **augenrules** will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

## System call structure

For performance (**man 7 audit.rules**) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      |  |  |
| v7               | <b>5.5 Implement Automated Configuration Monitoring Systems</b><br>Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.      |      |  |  |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1562, T1562.006                   | TA0005         | M1022              |

### *6.3.3.10 Ensure successful file system mounts are collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### **Description:**

Monitor the use of the **mount** system call. The **mount** (and **umount** ) system call controls the mounting and unmounting of file systems. The parameters below configure the system to create an audit record when the mount system call is used by a non-privileged user

#### **Rationale:**

It is highly unusual for a non privileged user to **mount** file systems to the system. While tracking **mount** commands gives the system administrator evidence that external media may have been mounted (based on a review of the source of the mount and confirming it's an external media type), it does not conclusively indicate that data was exported to the media. System administrators who wish to determine if data were exported, would also have to track successful **open**, **creat** and **truncate** system calls requiring write access to a file under the mount point of the external media file system. This could give a fair indication that a write occurred. The only way to truly prove it, would be to track successful writes to the external media. Tracking write system calls could quickly fill up the audit log and is not recommended. Recommendations on configuration options to track data export to media is beyond the scope of this document.

## Audit:

### On disk configuration

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
&&/ -F *arch=b(32|64)/ \
&&(/ -F *audit!=unset/||/ -F *audit!=-1/||/ -F *audit!=4294967295/) \
&&/ -F *audit>=${UID_MIN}/ \
&&/ -S/ \
&&/mount/ \
&&(/ key= *[:-~]* *$/||/ -k *[:-~]* *$/)" /etc/audit/rules.d/*.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S mount -F audit>=1000 -F audit!=unset -k mounts
-a always,exit -F arch=b32 -S mount -F audit>=1000 -F audit!=unset -k mounts
```

### Running configuration

Run the following command to check loaded rules:

```
# {
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
&&/ -F *arch=b(32|64)/ \
&&(/ -F *audit!=unset/||/ -F *audit!=-1/||/ -F *audit!=4294967295/) \
&&/ -F *audit>=${UID_MIN}/ \
&&/ -S/ \
&&/mount/ \
&&(/ key= *[:-~]* *$/||/ -k *[:-~]* *$/)" \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S mount -F audit>=1000 -F audit!=-1 -F key=mounts
-a always,exit -F arch=b32 -S mount -F audit>=1000 -F audit!=-1 -F key=mounts
```

## Remediation:

### Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful file system mounts.

*Example:*

```
# {
UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b32 -S mount -F auid>=UID_MIN -F auid!=unset -k
mounts
-a always,exit -F arch=b64 -S mount -F auid>=UID_MIN -F auid!=unset -k
mounts
" >> /etc/audit/rules.d/50-mounts.rules || printf "ERROR: Variable 'UID_MIN'
is unset.\n"
}
```

### Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230425  
RULE ID: SV-230425r627750  
STIG ID: RHEL-08-030302  
SEVERITY: CAT II

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

## Potential reboot required

If the auditing configuration is locked (**-e 2**), then **augenrules** will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

## System call structure

For performance (**man 7 audit.rules**) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      |  |  |
| v7               | <b>6.3 Enable Detailed Logging</b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.                                                                                |      |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0010  | M1034       |

### 6.3.3.11 *Ensure session initiation information is collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

Monitor session initiation events. The parameters in this section track changes to the files associated with session events.

- `/var/run/utmp` - tracks all currently logged in users.
- `/var/log/wtmp` - file tracks logins, logouts, shutdown, and reboot events.
- `/var/log/btmp` - keeps track of failed login attempts and can be read by entering the command `/usr/bin/last -f /var/log/btmp`.

All audit records will be tagged with the identifier "session."

#### **Rationale:**

Monitoring these files for changes could alert a system administrator to logins occurring at unusual hours, which could indicate intruder activity (i.e. a user logging in at a time when they do not normally log in).

## Audit:

### On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&(/\\var\\run\\utmp/ \
  |\\/var\\log\\wtmp/ \
  |\\/var\\log\\btmp/) \
&&/ +-p *wa/ \
&&(/ key= *[-~]* *$/||/ -k *[-~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k session
-w /var/log/btmp -p wa -k session
```

### Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&(/\\var\\run\\utmp/ \
  |\\/var\\log\\wtmp/ \
  |\\/var\\log\\btmp/) \
&&/ +-p *wa/ \
&&(/ key= *[-~]* *$/||/ -k *[-~]* *$/)'
```

Verify the output matches:

```
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k session
-w /var/log/btmp -p wa -k session
```



## Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor session initiation information.

*Example:*

```
# printf "  
-w /var/run/utmp -p wa -k session  
-w /var/log/wtmp -p wa -k session  
-w /var/log/btmp -p wa -k session  
" >> /etc/audit/rules.d/50-session.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot  
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3, AU-3

## Additional Information:

### Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### System call structure

For performance ([man 7 audit.rules](#)) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      |  |  |
| v7               | <b>4.9 <u>Log and Alert on Unsuccessful Administrative Account Login</u></b><br>Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.                                                                                                                 |      |  |  |
| v7               | <b>16.13 <u>Alert on Account Login Behavior Deviation</u></b><br>Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.                                                                                                                         |      |                                                                                     |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0001  | M1047       |

### *6.3.3.12 Ensure login and logout events are collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### **Description:**

Monitor login and logout events. The parameters below track changes to files associated with login/logout events.

- `/var/log/lastlog` - maintain records of the last time a user successfully logged in.
- `/var/run/faillock` - directory maintains records of login failures via the `pam_faillock` module.

#### **Rationale:**

Monitoring login/logout events could provide a system administrator with information associated with brute force attacks against user logins.

## Audit:

### On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&(/var/log/lastlog/ \
  ||/var/run/faillock/) \
&&/ +-p *wa/ \
&&(/ key= *[-~]* *$/||/ -k *[-~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /var/log/lastlog -p wa -k logins
-w /var/run/faillock -p wa -k logins
```

### Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&(/var/log/lastlog/ \
  ||/var/run/faillock/) \
&&/ +-p *wa/ \
&&(/ key= *[-~]* *$/||/ -k *[-~]* *$/)'
```

Verify the output matches:

```
-w /var/log/lastlog -p wa -k logins
-w /var/run/faillock -p wa -k logins
```

## Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor login and logout events.

*Example:*

```
# printf "
-w /var/log/lastlog -p wa -k logins
-w /var/run/faillock -p wa -k logins
" >> /etc/audit/rules.d/50-login.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230467  
Rule ID: SV-230467r627750  
STIG ID: RHEL-08-030600  
Severity: CAT II

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000473-GPOS-00218

### Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>4.9 <u>Log and Alert on Unsuccessful Administrative Account Login</u></b><br>Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.                                                                                                                 |      | ●    | ●    |
| v7               | <b>16.11 <u>Lock Workstation Sessions After Inactivity</u></b><br>Automatically lock workstation sessions after a standard period of inactivity.                                                                                                                                                      | ●    | ●    | ●    |
| v7               | <b>16.13 <u>Alert on Account Login Behavior Deviation</u></b><br>Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.                                                                                                                         |      |      | ●    |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1562, T1562.006                   | TA0001         | M1047              |

### *6.3.3.13 Ensure file deletion events by users are collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### **Description:**

Monitor the use of system calls associated with the deletion or renaming of files and file attributes. This configuration statement sets up monitoring for:

- **unlink** - remove a file
- **unlinkat** - remove a file attribute
- **rename** - rename a file
- **renameat** rename a file attribute system calls and tags them with the identifier "delete".

#### **Rationale:**

Monitoring these calls from non-privileged users could provide a system administrator with evidence that inappropriate removal of files and file attributes associated with protected files is occurring. While this audit option will look at all events, system administrators will want to look for specific privileged files that are being deleted or altered.

## Audit:

### On disk configuration

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
&&/ -F *arch=b(32|64)/ \
&&(/ -F *audit!=unset/||/ -F *audit!=-1/||/ -F *audit!=4294967295/) \
&&/ -F *audit>=${UID_MIN})/ \
&&/ -S/ \
&&(/unlink/||/rename/||/unlinkat/||/renameat/) \
&&(/ key= *[:-~]* *$/||/ -k *[:-~]* *$/)" /etc/audit/rules.d/*.rules \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S unlink,unlinkat,rename,renameat -F audit>=1000 -
F audit!=unset -k delete
-a always,exit -F arch=b32 -S unlink,unlinkat,rename,renameat -F audit>=1000 -
F audit!=unset -k delete
```

### Running configuration

Run the following command to check loaded rules:

```
# {
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
&&/ -F *arch=b(32|64)/ \
&&(/ -F *audit!=unset/||/ -F *audit!=-1/||/ -F *audit!=4294967295/) \
&&/ -F *audit>=${UID_MIN})/ \
&&/ -S/ \
&&(/unlink/||/rename/||/unlinkat/||/renameat/) \
&&(/ key= *[:-~]* *$/||/ -k *[:-~]* *$/)" \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S rename,unlink,unlinkat,renameat -F audit>=1000 -
F audit!=-1 -F key=delete
-a always,exit -F arch=b32 -S unlink,rename,unlinkat,renameat -F audit>=1000 -
F audit!=-1 -F key=delete
```



## Remediation:

### Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor file deletion events by users.

*Example:*

```
# {
UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b64 -S rename,unlink,unlinkat,renameat -F
auid>=${UID_MIN} -F auid!=unset -F key=delete
-a always,exit -F arch=b32 -S rename,unlink,unlinkat,renameat -F
auid>=${UID_MIN} -F auid!=unset -F key=delete
" >> /etc/audit/rules.d/50-delete.rules || printf "ERROR: Variable 'UID_MIN'
is unset.\n"
}
```

### Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230439  
Rule ID: SV-230439r810465  
STIG ID: RHEL-08-030361  
Severity: CAT II

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

## Potential reboot required

If the auditing configuration is locked (**-e 2**), then **augenrules** will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

## System call structure

For performance (**man 7 audit.rules**) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |                                                                                       |  |  |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0005  | M1047       |

### *6.3.3.14 Ensure events that modify the system's Mandatory Access Controls are collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

Monitor SELinux, an implementation of mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the `/etc/selinux/` and `/usr/share/selinux/` directories.

**Note:** If a different Mandatory Access Control method is used, changes to the corresponding directories should be audited.

#### **Rationale:**

Changes to files in the `/etc/selinux/` and `/usr/share/selinux/` directories could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.

## Audit:

### On disk configuration

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&(/\/etc\/selinux/ \
  ||\/usr\/share\/selinux/) \
&&/ +-p *wa/ \
&&(/ key= *![~]* *$/||/ -k *![~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /etc/selinux -p wa -k MAC-policy
-w /usr/share/selinux -p wa -k MAC-policy
```

### Running configuration

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&(/\/etc\/selinux/ \
  ||\/usr\/share\/selinux/) \
&&/ +-p *wa/ \
&&(/ key= *![~]* *$/||/ -k *![~]* *$/)'
```

Verify the output matches:

```
-w /etc/selinux -p wa -k MAC-policy
-w /usr/share/selinux -p wa -k MAC-policy
```

## Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify the system's Mandatory Access Controls.

*Example:*

```
# printf "
-w /etc/selinux -p wa -k MAC-policy
-w /usr/share/selinux -p wa -k MAC-policy
" >> /etc/audit/rules.d/50-MAC-policy.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3, CM-6

## Additional Information:

### Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <u>8.5 Collect Detailed Audit Logs</u><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      |    |    |
| v7               | <u>5.5 Implement Automated Configuration Monitoring Systems</u><br>Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.      |      |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0005  | M1022       |

### *6.3.3.15 Ensure successful and unsuccessful attempts to use the chcon command are collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### **Description:**

The operating system must generate audit records for successful/unsuccessful uses of the **chcon** command.

#### **Rationale:**

The **chcon** command is used to change file security context. Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

## Audit:

### On disk configuration

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
&&( / -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&/ -F *perm=x/ \
&&/ -F *path=/usr/bin/chcon/ \
&&( / key= *[-~]* *$/||/ -k *[-~]* *$/)" /etc/audit/rules.d/*.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F auid!=unset
-k perm_chng
```

### Running configuration

Run the following command to check loaded rules:

```
# {
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
&&( / -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&/ -F *perm=x/ \
&&/ -F *path=/usr/bin/chcon/ \
&&( / key= *[-~]* *$/||/ -k *[-~]* *$/)" \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -S all -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F
auid!=-1 -F key=perm_chng
```

## Remediation:

### Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful and unsuccessful attempts to use the `chcon` command.

*Example:*

```
# {
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && printf "
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k perm_chng
" >> /etc/audit/rules.d/50-perm_chng.rules || printf "ERROR: Variable
'UID_MIN' is unset.\n"
}
```

### Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230419  
Rule ID: SV-230419r627750  
STIG ID: RHEL-08-030260  
Severity: CAT II

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000468-GPOS-00212, SRG-OS-000471-GPOS-00215

## Potential reboot required

If the auditing configuration is locked (**-e 2**), then **augenrules** will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

## System call structure

For performance (**man 7 audit.rules**) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                 | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.2 Collect Audit Logs</b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0005  | M1022       |

### *6.3.3.16 Ensure successful and unsuccessful attempts to use the setfacl command are collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

The operating system must generate audit records for successful/unsuccessful uses of the **setfacl** command

#### **Rationale:**

This utility sets Access Control Lists (ACLs) of files and directories. Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

## Audit:

### On disk configuration

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
&&( / -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&/ -F *perm=x/ \
&&/ -F *path=/usr/bin/setfacl/ \
&&( / key= *[:-~]* *$/||/ -k *[:-~]* *$/)" /etc/audit/rules.d/*.rules ||
  printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F
auid!=unset -k perm_chng
```

### Running configuration

Run the following command to check loaded rules:

```
# {
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
&&( / -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&/ -F *perm=x/ \
&&/ -F *path=/usr/bin/setfacl/ \
&&( / key= *[:-~]* *$/||/ -k *[:-~]* *$/)" \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -S all -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F
auid!=-1 -F key=perm_chng
```

## Remediation:

### Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful and unsuccessful attempts to use the `setfacl` command.

*Example:*

```
# {
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && printf "
-a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k perm_chng
" >> /etc/audit/rules.d/50-perm_chng.rules || printf "ERROR: Variable
'UID_MIN' is unset.\n"
}
```

### Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230435  
Rule ID: SV-230435r627750  
STIG ID: RHEL-08-030330  
Severity: CAT II

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

## Potential reboot required

If the auditing configuration is locked (**-e 2**), then **augenrules** will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

## System call structure

For performance (**man 7 audit.rules**) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                 | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.2 Collect Audit Logs</b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0005  | M1022       |

### *6.3.3.17 Ensure successful and unsuccessful attempts to use the chacl command are collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### **Description:**

The operating system must generate audit records for successful/unsuccessful uses of the **chacl** command.

**chacl** is an IRIX-compatibility command, and is maintained for those users who are familiar with its use from either XFS or IRIX.

#### **Rationale:**

**chacl** changes the ACL(s) for a file or directory. Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000466-GPOS-00210

## Audit:

### On disk configuration

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
&&( / -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&/ -F *perm=x/ \
&&/ -F *path=/usr/bin/chacl/ \
&&( / key= *[-~]* *$/||/ -k *[-~]* *$/)" /etc/audit/rules.d/*.rules \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F auid!=unset
-k perm_chng
```

### Running configuration

Run the following command to check loaded rules:

```
# {
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
&&( / -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&/ -F *perm=x/ \
&&/ -F *path=/usr/bin/chacl/ \
&&( / key= *[-~]* *$/||/ -k *[-~]* *$/)" \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -S all -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F
auid!=-1 -F key=perm_chng
```

## Remediation:

### Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful and unsuccessful attempts to use the `chac1` command.

*Example:*

```
# {
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && printf "
-a always,exit -F path=/usr/bin/chac1 -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k perm_chng
" >> /etc/audit/rules.d/50-perm_chng.rules || printf "ERROR: Variable
'UID_MIN' is unset.\n"
}
```

### Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 Rev. 5: AU-2, AU-12, SI-5
2. NIST SP 800-53A :: AU-12.1 (ii)



## Additional Information:

### Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230464  
Rule ID: SV-230464r627750  
STIG ID: RHEL-08-030570  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0005  | M1022       |

### *6.3.3.18 Ensure successful and unsuccessful attempts to use the usermod command are collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### **Description:**

The operating system must generate audit records for successful/unsuccessful uses of the **usermod** command.

#### **Rationale:**

The **usermod** command modifies the system account files to reflect the changes that are specified on the command line. Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

## Audit:

### On disk configuration

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
&&( / -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&/ -F *perm=x/ \
&&/ -F *path=/usr/sbin/usermod/ \
&&( / key= *[-~]* *$/||/ -k *[-~]* *$/)" /etc/audit/rules.d/*.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F
auid!=unset -k usermod
```

### Running configuration

Run the following command to check loaded rules:

```
# {
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
&&( / -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&/ -F *perm=x/ \
&&/ -F *path=/usr/sbin/usermod/ \
&&( / key= *[-~]* *$/||/ -k *[-~]* *$/)" \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -S all -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F
auid!=-1 -F key=usermod
```

## Remediation:

### Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful and unsuccessful attempts to use the `usermod` command.

*Example:*

```
# {
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && printf "
-a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k usermod
" >> /etc/audit/rules.d/50-usermod.rules || printf "ERROR: Variable 'UID_MIN'
is unset.\n"
}
```

### Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230463  
Rule ID: SV-230463r627750  
STIG ID: RHEL-08-030560  
Severity: CAT II

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000466-GPOS-00210

## Potential reboot required

If the auditing configuration is locked (**-e 2**), then **augenrules** will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

## System call structure

For performance (**man 7 audit.rules**) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                 | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.2 Collect Audit Logs</b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |  |  |  |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.006            | TA0005  | M1022       |

### *6.3.3.19 Ensure kernel module loading unloading and modification is collected (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### **Description:**

Monitor the loading and unloading of kernel modules. All the loading / listing / dependency checking of modules is done by **kmod** via symbolic links.

The following system calls control loading and unloading of modules:

- **init\_module** - load a module
- **finit\_module** - load a module (used when the overhead of using cryptographically signed modules to determine the authenticity of a module can be avoided)
- **delete\_module** - delete a module
- **create\_module** - create a loadable module entry
- **query\_module** - query the kernel for various bits pertaining to modules

Any execution of the loading and unloading module programs and system calls will trigger an audit record with an identifier of **modules**.

#### **Rationale:**

Monitoring the use of all the various ways to manipulate kernel modules could provide system administrators with evidence that an unauthorized change was made to a kernel module, possibly compromising the security of the system.

## Audit:

### On disk configuration

Run the following script to check the on disk rules:

```
#!/usr/bin/env bash

{
  awk '/^ *-a *always,exit/ \
    &&/ -F *arch=b(32|64)/ \
    &&/ -F auid!=unset/||/ -F auid!=-1/||/ -F auid!=4294967295/) \
    &&/ -S/ \
    &&/init_module/ \
      ||/finit_module/ \
      ||/delete_module/ \
      ||/create_module/ \
      ||/query_module/) \
    &&/ key= *[:-~]* *$/||/ -k *[:-~]* *$/)' /etc/audit/rules.d/*.rules

  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
    &&/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
    &&/ -F *auid>=${UID_MIN}/ \
    &&/ -F *perm=x/ \
    &&/ -F *path=/usr/bin/kmod/ \
    &&/ key= *[:-~]* *$/||/ -k *[:-~]* *$/)" /etc/audit/rules.d/*.rules \
    || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S
init_module,finit_module,delete_module,create_module,query_module -F
auid>=1000 -F auid!=unset -k kernel_modules
-a always,exit -F path=/usr/bin/kmod -F perm=x -F auid>=1000 -F auid!=unset -
k kernel_modules
```

### Running configuration

Run the following script to check loaded rules:

```
#!/usr/bin/env bash

{
  auditctl -l | awk '/^ *-a *always,exit/ \
&&/ -F *arch=b(32|64)/ \
&&/ -F auid!=unset/||/ -F auid!=-1/||/ -F auid!=4294967295/) \
&&/ -S/ \
&&/init_module/ \
  ||/finit_module/ \
  ||/delete_module/ \
  ||/create_module/ \
  ||/query_module/) \
&&/ key= *[:-~]* *$/||/ -k *[:-~]* *$/)'

  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
&&/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&/ -F *auid>=${UID_MIN}/ \
&&/ -F *perm=x/ \
&&/ -F *path=/usr/bin/kmod/ \
&&/ key= *[:-~]* *$/||/ -k *[:-~]* *$/)" \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output includes:

```
-a always,exit -F arch=b64 -S
create_module,init_module,delete_module,query_module,finit_module -F
auid>=1000 -F auid!=-1 -F key=kernel_modules
-a always,exit -S all -F path=/usr/bin/kmod -F perm=x -F auid>=1000 -F
auid!=-1 -F key=kernel_modules
```

## Symlink audit

Run the following script to audit if the symlinks **kmod** accepts are indeed pointing at it:

```
#!/usr/bin/env bash

{
  a_files=("/usr/sbin/lsmmod" "/usr/sbin/rmmmod" "/usr/sbin/inmod"
"/usr/sbin/modinfo" "/usr/sbin/modprobe" "/usr/sbin/depmod")
  for l_file in "${a_files[@]}; do
    if [ "$(readlink -f "$l_file")" = "$(readlink -f /bin/kmod)" ]; then
      printf "OK: \"$l_file\"\n"
    else
      printf "Issue with symlink for file: \"$l_file\"\n"
    fi
  done
}
```

Verify the output states **OK**. If there is a symlink pointing to a different location it should be investigated



## Remediation:

### Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor kernel module modification.

*Example:*

```
#!/usr/bin/env bash

{
  UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b64 -S
init_module,fininit_module,delete_module,create_module,query_module -F
auid>=${UID_MIN} -F auid!=unset -k kernel_modules
-a always,exit -F path=/usr/bin/kmod -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k kernel_modules
" >> /etc/audit/rules.d/50-kernel_modules.rules || printf "ERROR: Variable
'UID_MIN' is unset.\n"
}
```

### Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230438  
Rule ID: SV-230438r810464  
STIG ID: RHEL-08-030360  
Severity: CAT II

Vul ID: V-230446  
Rule ID: SV-230446r627750  
STIG ID: RHEL-08-030390  
Severity: CAT II

Vul ID: V-230465  
Rule ID: SV-230465r627750  
STIG ID: RHEL-08-030580  
Severity: CAT II

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

## Potential reboot required

If the auditing configuration is locked (**-e 2**), then **augenrules** will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

## System call structure

For performance (**man 7 audit.rules**) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1562, T1562.006                   | TA0004         | M1047              |

### 6.3.3.20 Ensure the audit configuration is immutable (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation
- STIG

#### Description:

Set system audit so that audit rules cannot be modified with `auditctl`. Setting the flag "-e 2" forces audit to be put in immutable mode. Audit changes can only be made on system reboot.

**Note:** This setting will require the system to be rebooted to update the active `auditd` configuration settings.

#### Rationale:

In immutable mode, unauthorized users cannot execute changes to the audit system to potentially hide malicious activity and then put the audit rules back. Users would most likely notice a system reboot and that could alert administrators of an attempt to make unauthorized audit changes.

#### Audit:

Run the following command and verify output matches:

```
# grep -Ph -- '^h*-e\h+2\b' /etc/audit/rules.d/*.rules | tail -1  
-e 2
```

## Remediation:

Edit or create the file `/etc/audit/rules.d/99-finalize.rules` and add the line `-e 2` at the end of the file:

*Example:*

```
# printf '\n%s' "-e 2" >> /etc/audit/rules.d/99-finalize.rules
```

## Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot  
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-9
2. NIST SP 800-53A :: AU-9.1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230402  
Rule ID: SV-230402r627750  
STIG ID: RHEL-08-030121  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                        |  |  |  |
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |                                                                                     |  |  |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         |  |  |  |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.                                                                                |                                                                                     |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1562, T1562.001            | TA0005  | M1022       |

### 6.3.3.21 *Ensure the running and on disk configuration is the same (Manual)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

The Audit system have both on disk and running configuration. It is possible for these configuration settings to differ.

**Note:** Due to the limitations of `augenrules` and `auditctl`, it is not absolutely guaranteed that loading the rule sets via `augenrules --load` will result in all rules being loaded or even that the user will be informed if there was a problem loading the rules.

#### **Rationale:**

Configuration differences between what is currently running and what is on disk could cause unexpected problems or may give a false impression of compliance requirements.

#### **Audit:**

##### **Merged rule sets**

Ensure that all rules in `/etc/audit/rules.d` have been merged into `/etc/audit/audit.rules`:

```
# augenrules --check
/usr/sbin/augenrules: No change
```

Should there be any drift, run `augenrules --load` to merge and load all rules.

#### **Remediation:**

If the rules are not aligned across all three () areas, run the following command to merge and load all rules:

```
# augenrules --load
```

Check if reboot is required.

```
if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then echo "Reboot required to load rules"; fi
```

#### **References:**

1. NIST SP 800-53 Rev. 5: AU-3

## Additional Information:

### Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      |  |  |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.                                                                                |      |  |  |



### 6.3.3.22 *Ensure successful and unsuccessful attempts to use the su command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful uses of the su command must generate an audit record.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "su" command allows a user to run commands with a substitute user and group ID.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000064-GPOS-0003, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000466-GPOS-00210

#### **Audit:**

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "su" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w /usr/bin/su /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/bin/su -F perm=x -F auid>=1000 -F auid!=unset -k  
privileged-priv_change
```

If the command does not return a line, or the line is commented out, this is a finding.

## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the **su** command by adding or updating the following rule in a **.rules** file in the **/etc/audit/rules.d/** directory:

```
-a always,exit -F path=/usr/bin/su -F perm=x -F auid>=1000 -F auid!=unset -k privileged-priv_change
```

### Example:

```
#!/usr/bin/env bash

{
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \
        "-a always,exit -F path=/usr/bin/su -F perm=x -F auid>=${UID_MIN} -F auid!=unset -k privileged-priv_change" \
        >> /etc/audit/rules.d/50-privileged-priv_change.rules || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230412  
Rule ID: SV-230412r627750  
STIG ID: RHEL-08-030190  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      |  |  |
| v7               | <b>4.9 <u>Log and Alert on Unsuccessful Administrative Account Login</u></b><br>Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.                                                                                                                 |      |  |  |

### 6.3.3.23 *Ensure successful and unsuccessful attempts to use the sudo command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful uses of the sudo command must generate an audit record.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "sudo" command allows a permitted user to execute a command as the superuser or another user, as specified by the security policy.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000466-GPOS-00210

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of the "sudo" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w sudo /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F auid!=unset -
k priv_cmd
```

If the command does not return a line, or the line is commented out, this is a finding.

## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the **sudo** command by adding or updating the following rule in a **.rules** file in the **/etc/audit/rules.d/** directory:

```
-a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F auid!=unset -k priv_cmd
```

### Example:

```
#!/usr/bin/env bash

{
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \
        "-a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=${UID_MIN} -F auid!=unset -k priv_cmd" \
        >> /etc/audit/rules.d/50-priv_cmd.rules || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 Revision 5 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230462  
Rule ID: SV-230462r627750  
STIG ID: RHEL-08-030550  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>4.9 <u>Log and Alert on Unsuccessful Administrative Account Login</u></b><br>Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.                                                                                                                 |      | ●    | ●    |

### 6.3.3.24 Ensure successful and unsuccessful attempts to use the chsh command are collected (Automated)

#### Profile Applicability:

- STIG

#### Description:

Successful/unsuccessful uses of the chsh command must generate an audit record.

#### Rationale:

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "chsh" command is used to change the login shell.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

#### Audit:

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "chsh" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w chsh /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F auid!=unset -  
k priv_cmd
```

If the command does not return a line, or the line is commented out, this is a finding.

## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "chsh" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F auid!=unset -k priv_cmd
```

The audit daemon must be restarted for the changes to take effect.

Configure the audit system to generate an audit event for any successful/unsuccessful use of the **chsh** command by adding or updating the following rule in a **.rules** file in the **/etc/audit/rules.d/** directory:

```
-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F auid!=unset -k priv_cmd
```

### Example:

```
#!/usr/bin/env bash

{
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \
        "-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=${UID_MIN} -F auid!=unset -k priv_cmd" \
        >> /etc/audit/rules.d/50-priv_cmd.rules || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 Revision 5 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230448  
Rule ID: SV-230448r627750  
STIG ID: RHEL-08-030410  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

### 6.3.3.25 *Ensure successful and unsuccessful attempts to use the crontab command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful uses of the crontab command must generate an audit record.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "crontab" command is used to maintain crontab files for individual users. Crontab is the program used to install, remove, or list the tables used to drive the cron daemon. This is similar to the task scheduler used in other operating systems.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of the "crontab" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w crontab /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-crontab
```

If the command does not return a line, or the line is commented out, this is a finding.

## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the **crontab** command by adding or updating the following rule in a **.rules** file in the **/etc/audit/rules.d/** directory:

```
-a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-crontab
```

### Example:

```
#!/usr/bin/env bash  
  
{  
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)  
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \  
        "-a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=${UID_MIN} -F  
auid!=unset -k privileged-crontab" \  
        >> /etc/audit/rules.d/50-privileged-crontab.rules || printf "ERROR:  
Variable 'UID_MIN' is unset.\n"  
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot  
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230447  
Rule ID: SV-230447r627750  
STIG ID: RHEL-08-030400  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

### 6.3.3.26 *Ensure successful and unsuccessful attempts to use the gpasswd command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful uses of the gpasswd command must generate an audit record.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "gpasswd" command is used to administer /etc/group and /etc/gshadow. Every group can have administrators, members and a password.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of the "gpasswd" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w gpasswd /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-gpasswd
```

If the command does not return a line, or the line is commented out, this is a finding.

## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the **gpasswd** command by adding or updating the following rule in a **.rules** file in the **/etc/audit/rules.d/** directory:

```
-a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-gpasswd
```

### Example:

```
#!/usr/bin/env bash  
  
{  
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)  
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \  
        "-a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=${UID_MIN} -F  
auid!=unset -k privileged-gpasswd" \  
        >> /etc/audit/rules.d/50-privileged-gpasswd.rules || printf "ERROR:  
Variable 'UID_MIN' is unset.\n"  
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot  
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230444  
Rule ID: SV-230444r627750  
STIG ID: RHEL-08-030370  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

### 6.3.3.27 *Ensure successful and unsuccessful attempts to use the newgrp command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful uses of the newgrp command must generate an audit record.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "newgrp" command is used to change the current group ID during a login session.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

#### **Audit:**

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "newgrp" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w newgrp /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F auid!=unset  
-k priv_cmd
```

If the command does not return a line, or the line is commented out, this is a finding.



## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the **newgrp** command by adding or updating the following rule in a **.rules** file in the **/etc/audit/rules.d/** directory:

```
-a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F auid!=unset  
-k priv_cmd
```

### Example:

```
#!/usr/bin/env bash  
  
{  
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)  
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \  
        "-a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=${UID_MIN} -F  
auid!=unset -k priv_cmd" \  
        >> /etc/audit/rules.d/50-priv_cmd.rules || printf "ERROR: Variable  
'UID_MIN' is unset.\n"  
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot  
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230437  
Rule ID: SV-230437r627750  
STIG ID: RHEL-08-030350  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

### 6.3.3.28 *Ensure successful and unsuccessful attempts to use the pam\_timestamp\_check command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful uses of the pam\_timestamp\_check command must generate an audit record.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "pam\_timestamp\_check" command is used to check if the default timestamp is valid.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of the "pam\_timestamp\_check" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w pam_timestamp_check /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/sbin/pam_timestamp_check -F perm=x -F auid>=1000  
-F auid!=unset -k privileged-pam_timestamp_check
```

If the command does not return a line, or the line is commented out, this is a finding.

## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the `pam_timestamp_check` command by adding or updating the following rule in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
-a always,exit -F path=/usr/sbin/pam_timestamp_check -F perm=x -F auid>=1000  
-F auid!=unset -k privileged-pam_timestamp_check
```

### Example:

```
#!/usr/bin/env bash  
  
{  
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)  
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \  
        "-a always,exit -F path=/usr/sbin/pam_timestamp_check -F perm=x -F  
auid>=${UID_MIN} -F auid!=unset -k privileged-pam_timestamp_check" \  
        >> /etc/audit/rules.d/50-privileged-pam_timestamp_check || printf "ERROR:  
Variable 'UID_MIN' is unset.\n"  
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot  
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 Revision 5 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230436  
Rule ID: SV-230436r627750  
STIG ID: RHEL-08-030340  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

### 6.3.3.29 *Ensure successful and unsuccessful attempts to use the ssh-keysign command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful uses of the ssh-keysign must generate an audit record.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "ssh-keysign" program is an SSH helper program for host-based authentication.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

#### **Audit:**

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "ssh-keysign" by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep ssh-keysign /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/libexec/openssh/ssh-keysign -F perm=x -F  
auid>=1000 -F auid!=unset -k privileged-ssh
```

If the command does not return a line, or the line is commented out, this is a finding.

## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the **ssh-keysign** command by adding or updating the following rule in a **.rules** file in the **/etc/audit/rules.d/** directory:

```
-a always,exit -F path=/usr/libexec/openssh/ssh-keysign -F perm=x -F  
audit>=1000 -F audit!=unset -k privileged-ssh
```

### Example:

```
#!/usr/bin/env bash  
  
{  
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)  
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \  
        "-a always,exit -F path=/usr/libexec/openssh/ssh-keysign -F perm=x -F  
audit>=${UID_MIN} -F audit!=unset -k privileged-ssh" \  
        >> /etc/audit/rules.d/50-privileged-ssh.rules || printf "ERROR: Variable  
'UID_MIN' is unset.\n"  
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot  
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 Revision 5 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230434  
Rule ID: SV-230434r744002  
STIG ID: RHEL-08-030320  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |



### 6.3.3.30 *Ensure successful and unsuccessful attempts to use the unix\_chkpwd command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful uses of unix\_chkpwd must generate an audit record.

#### **Rationale:**

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "unix\_chkpwd" command is a helper program for the pam\_unix module that verifies the password of the current user. It also checks password and account expiration dates in shadow. It is not intended to be run directly from the command line and logs a security violation if done so.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of "unix\_chkpwd" by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "unix_chkpwd" /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/sbin/unix_chkpwd -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the `unix_chkpwd` command by adding or updating the following rule in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
-a always,exit -F path=/usr/sbin/unix_chkpwd -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

### Example:

```
#!/usr/bin/env bash

{
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \
        "-a always,exit -F path=/usr/sbin/unix_chkpwd -F perm=x -F
auid>=${UID_MIN} -F auid!=unset -k privileged-unix-update" \
        >> /etc/audit/rules.d/50-privileged-unix-update.rules || printf "ERROR:
Variable 'UID_MIN' is unset.\n"
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230433  
Rule ID: SV-230433r627750  
STIG ID: RHEL-08-030317  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

### 6.3.3.31 *Ensure successful and unsuccessful attempts to use the setsebool command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful uses of setsebool must generate an audit record.

#### **Rationale:**

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "setsebool" command sets the current state of a particular SELinux boolean or a list of booleans to a given value.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of "setsebool" by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "setsebool" /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/setsebool -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the **setsebool** command by adding or updating the following rule in a **.rules** file in the **/etc/audit/rules.d/** directory:

```
-a always,exit -F path=/usr/sbin/setsebool -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-unix-update
```

### Example:

```
#!/usr/bin/env bash  
  
{  
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)  
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \  
        "-a always,exit -F path=/usr/sbin/setsebool -F perm=x -F auid>=${UID_MIN}  
-F auid!=unset -k privileged-unix-update" \  
        >> /etc/audit/rules.d/50-privileged-unix-update.rules || printf "ERROR:  
Variable 'UID_MIN' is unset.\n"  
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot  
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230432  
Rule ID: SV-230432r627750  
STIG ID: RHEL-08-030316  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

### 6.3.3.32 *Ensure successful and unsuccessful attempts to use the userhelper command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful uses of userhelper must generate an audit record.

#### **Rationale:**

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "userhelper" command is not intended to be run interactively. "Userhelper" provides a basic interface to change a user's password, gecol information, and shell. The main difference between this program and its traditional equivalents (passwd, chfn, chsh) is that prompts are written to standard out to make it easy for a graphical user interface wrapper to interface to it as a child process.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of "userhelper" by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "userhelper" /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/userhelper -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the **userhelper** command by adding or updating the following rule in a **.rules** file in the **/etc/audit/rules.d/** directory:

```
-a always,exit -F path=/usr/sbin/userhelper -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

### Example:

```
#!/usr/bin/env bash

{
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \
        "-a always,exit -F path=/usr/sbin/userhelper -F perm=x -F auid>=${UID_MIN}
-F auid!=unset -k privileged-unix-update" \
        >> /etc/audit/rules.d/50-privileged-unix-update.rules || printf "ERROR:
Variable 'UID_MIN' is unset.\n"
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 4 Benchmark Date: 24 Apr 2024

Vul ID: V-230431  
Rule ID: SV-230431r627750  
STIG ID: RHEL-08-030315  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

### 6.3.3.33 *Ensure successful and unsuccessful attempts to use the setfiles command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful uses of setfiles must generate an audit record.

#### **Rationale:**

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "setfiles" command is primarily used to initialize the security context fields (extended attributes) on one or more filesystems (or parts of them). Usually it is initially run as part of the SELinux installation process (a step commonly known as labeling).

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of "setfiles" by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "setfiles" /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/sbin/setfiles -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the **setfiles** command by adding or updating the following rule in a **.rules** file in the **/etc/audit/rules.d/** directory:

```
-a always,exit -F path=/usr/sbin/setfiles -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-unix-update
```

### Example:

```
#!/usr/bin/env bash  
  
{  
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)  
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \  
        "-a always,exit -F path=/usr/sbin/setfiles -F perm=x -F auid>=${UID_MIN} -  
F auid!=unset -k privileged-unix-update" \  
        >> /etc/audit/rules.d/50-privileged-unix-update.rules || printf "ERROR:  
Variable 'UID_MIN' is unset.\n"  
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot  
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230430  
Rule ID: SV-230430r627750  
STIG ID: RHEL-08-030314  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

### 6.3.3.34 *Ensure successful and unsuccessful attempts to use the semanage command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful uses of semanage must generate an audit record.

#### **Rationale:**

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "semanage" command is used to configure certain elements of SELinux policy without requiring modification to or recompilation from policy sources.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of "semanage" by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "semanage" /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/sbin/semanage -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the **semanage** command by adding or updating the following rule in a **.rules** file in the **/etc/audit/rules.d/** directory:

```
-a always,exit -F path=/usr/sbin/semanage -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-unix-update
```

### Example:

```
#!/usr/bin/env bash  
  
{  
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)  
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \  
        "-a always,exit -F path=/usr/sbin/semanage -F perm=x -F auid>=${UID_MIN} -  
F auid!=unset -k privileged-unix-update" \  
        >> /etc/audit/rules.d/50-privileged-unix-update.rules || printf "ERROR:  
Variable 'UID_MIN' is unset.\n"  
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot  
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230429  
Rule ID: SV-230429r627750  
STIG ID: RHEL-08-030313  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

### 6.3.3.35 *Ensure successful and unsuccessful attempts to use the postqueue command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful uses of postqueue must generate an audit record.

#### **Rationale:**

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "postqueue" command implements the Postfix user interface for queue management.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of "postqueue" by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "postqueue" /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/sbin/postqueue -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.



## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the `postqueue` command by adding or updating the following rule in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
-a always,exit -F path=/usr/sbin/postqueue -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-unix-update
```

### Example:

```
#!/usr/bin/env bash  
  
{  
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)  
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \  
        "-a always,exit -F path=/usr/sbin/postqueue -F perm=x -F auid>=${UID_MIN}  
-F auid!=unset -k privileged-unix-update" \  
        >> /etc/audit/rules.d/50-privileged-unix-update.rules || printf "ERROR:  
Variable 'UID_MIN' is unset.\n"  
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot  
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230428  
Rule ID: SV-230428r627750  
STIG ID: RHEL-08-030312  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |                                                                                     |  |  |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         |  |  |  |

### 6.3.3.36 *Ensure successful and unsuccessful attempts to use the postdrop command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful uses of postdrop must generate an audit record.

#### **Rationale:**

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. The "postdrop" command creates a file in the maildrop directory and copies its standard input to the file.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of "postdrop" by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "postdrop" /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/sbin/postdrop -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "postdrop" by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/postdrop -F perm=x -F auid>=1000 -F auid!=unset -k privileged-unix-update
```

The audit daemon must be restarted for the changes to take effect.

Configure the audit system to generate an audit event for any successful/unsuccessful use of the **postdrop** command by adding or updating the following rule in a **.rules** file in the **/etc/audit/rules.d/** directory:

```
-a always,exit -F path=/usr/sbin/postdrop -F perm=x -F auid>=1000 -F auid!=unset -k privileged-unix-update
```

### Example:

```
#!/usr/bin/env bash

{
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \
        "-a always,exit -F path=/usr/sbin/postdrop -F perm=x -F auid>=${UID_MIN} -F auid!=unset -k privileged-unix-update" \
        >> /etc/audit/rules.d/50-privileged-unix-update.rules || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230427  
Rule ID: SV-230427r627750  
STIG ID: RHEL-08-030311  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

### 6.3.3.37 *Ensure successful and unsuccessful attempts to use the unix\_update command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful uses of the unix\_update must generate an audit record.

#### **Rationale:**

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise. "Unix\_update" is a helper program for the "pam\_unix" module that updates the password for a given user. It is not intended to be run directly from the command line and logs a security violation if done so.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of the "unix\_update" by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w "unix_update" /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/unix_update -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the `unix_update` command by adding or updating the following rule in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
-a always,exit -F path=/usr/sbin/unix_update -F perm=x -F auid>=1000 -F auid!=unset -k privileged-unix-update
```

### Example:

```
#!/usr/bin/env bash

{
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \
        "-a always,exit -F path=/usr/sbin/unix_update -F perm=x -F auid>=${UID_MIN} -F auid!=unset -k privileged-unix-update" \
        >> /etc/audit/rules.d/50-privileged-unix-update.rules || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230426  
Rule ID: SV-230426r627750  
STIG ID: RHEL-08-030310  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |



### 6.3.3.38 *Ensure successful and unsuccessful attempts to use the umount command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful uses of the umount command must generate an audit record.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "umount" command is used to unmount a filesystem.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of the "umount" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w /usr/bin/umount /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/bin/umount -F perm=x -F auid>=1000 -F auid!=unset  
-k privileged-mount
```

If the command does not return a line, or the line is commented out, this is a finding.

## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the **umount** command by adding or updating the following rule in a **.rules** file in the **/etc/audit/rules.d/** directory:

```
-a always,exit -F path=/usr/bin/umount -F perm=x -F auid>=1000 -F auid!=unset  
-k privileged-mount
```

### Example:

```
#!/usr/bin/env bash  
  
{  
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)  
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \  
        "-a always,exit -F path=/usr/bin/umount -F perm=x -F auid>=${UID_MIN} -F  
auid!=unset -k privileged-mount" \  
        >> /etc/audit/rules.d/50-privileged-mount.rules || printf "ERROR: Variable  
'UID_MIN' is unset.\n"  
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot  
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230424  
Rule ID: SV-230424r627750  
STIG ID: RHEL-08-030301  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

### 6.3.3.39 *Ensure successful and unsuccessful attempts to use the mount command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful uses of the mount command must generate an audit record.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "mount" command is used to mount a filesystem.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of the "mount" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w /usr/bin/mount /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/bin/mount -F perm=x -F auid>=1000 -F auid!=unset  
-k privileged-mount
```

If the command does not return a line, or the line is commented out, this is a finding.

## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the **mount** command by adding or updating the following rule in a **.rules** file in the **/etc/audit/rules.d/** directory:

```
-a always,exit -F path=/usr/bin/mount -F perm=x -F auid>=1000 -F auid!=unset  
-k privileged-mount
```

### Example:

```
#!/usr/bin/env bash  
  
{  
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)  
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \  
        "-a always,exit -F path=/usr/bin/mount -F perm=x -F auid>=${UID_MIN} -F  
auid!=unset -k privileged-mount" \  
        >> /etc/audit/rules.d/50-privileged-mount.rules || printf "ERROR: Variable  
'UID_MIN' is unset.\n"  
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot  
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230423  
Rule ID: SV-230423r627750  
STIG ID: RHEL-08-030300  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

### 6.3.3.40 *Ensure successful and unsuccessful attempts to use the ssh-agent command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful uses of the ssh-agent must generate an audit record.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "ssh-agent" is a program to hold private keys used for public key authentication.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

#### **Audit:**

Verify the operating system generates an audit record when successful/unsuccessful attempts to use the "ssh-agent" by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep ssh-agent /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/bin/ssh-agent -F perm=x -F auid>=1000 -F  
auid!=unset -k privileged-ssh
```

If the command does not return a line, or the line is commented out, this is a finding.

## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the **ssh-agent** command by adding or updating the following rule in a **.rules** file in the **/etc/audit/rules.d/** directory:

```
-a always,exit -F path=/usr/bin/ssh-agent -F perm=x -F auid>=1000 -F auid!=unset -k privileged-ssh
```

### Example:

```
#!/usr/bin/env bash

{
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \
        "-a always,exit -F path=/usr/bin/ssh-agent -F perm=x -F auid>=${UID_MIN} -F auid!=unset -k privileged-ssh" \
        >> /etc/audit/rules.d/50-privileged-ssh.rules || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230421  
Rule ID: SV-230421r627750  
STIG ID: RHEL-08-030280  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

### 6.3.3.41 *Ensure successful and unsuccessful attempts to use the passwd command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful uses of the passwd command must generate an audit record.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "passwd" command is used to change passwords for user accounts.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of the "passwd" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w passwd /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=unset  
-k privileged-passwd
```

If the command does not return a line, or the line is commented out, this is a finding.

## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the `passwd` command by adding or updating the following rule in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=unset  
-k privileged-passwd
```

### Example:

```
#!/usr/bin/env bash  
  
{  
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)  
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \  
        "-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=${UID_MIN} -F  
auid!=unset -k privileged-passwd" \  
        >> /etc/audit/rules.d/50-privileged-passwd.rules || printf "ERROR:  
Variable 'UID_MIN' is unset.\n"  
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot  
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230422  
Rule ID: SV-230422r627750  
STIG ID: RHEL-08-030290  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

### 6.3.3.42 *Ensure successful and unsuccessful attempts to use the chage command are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful uses of the chage command must generate an audit record.

#### **Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter). The "chage" command is used to change or view user password expiry information.

When a user logs on, the AUID is set to the UID of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to "-1". The AUID representation is an unsigned 32-bit integer, which equals "4294967295". The audit system interprets "-1", "4294967295", and "unset" in the same way.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000468-GPOS-00212, SRG-OS-000471-GPOS-00215

#### **Audit:**

Verify that an audit event is generated for any successful/unsuccessful use of the "chage" command by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w chage /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F auid!=unset  
-k privileged-chage
```

If the command does not return a line, or the line is commented out, this is a finding.

## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the **chage** command by adding or updating the following rule in a **.rules** file in the **/etc/audit/rules.d/** directory:

```
-a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F auid!=unset  
-k privileged-chage
```

### Example:

```
#!/usr/bin/env bash  
  
{  
    UID_MIN=$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)  
    [ -n "${UID_MIN}" ] && printf '\n%s\n' \  
        "-a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=${UID_MIN} -F  
auid!=unset -k privileged-chage" \  
        >> /etc/audit/rules.d/50-privileged-chage.rules || printf "ERROR: Variable  
'UID_MIN' is unset.\n"  
}
```

Run the following command to merge and load the rules into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot  
required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230418  
Rule ID: SV-230418r627750  
STIG ID: RHEL-08-030250  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1 | IG 2 | IG 3 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

### 6.3.3.43 *Ensure the audit system prevents unauthorized changes to logon UIDs (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The audit system must protect logon UIDs from unauthorized change.

#### **Rationale:**

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit system activity.

In immutable mode, unauthorized users cannot execute changes to the audit system to potentially hide malicious activity and then put the audit rules back. A system reboot would be noticeable and a system administrator could then investigate the unauthorized changes.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

#### **Audit:**

Verify the audit system prevents unauthorized changes to logon UIDs with the following command:

```
# grep -i immutable /etc/audit/audit.rules  
  
--loginuid-immutable
```

If the login UIDs are not set to be immutable by adding the "--loginuid-immutable" option to the "/etc/audit/audit.rules", this is a finding.

#### **Example:**

```
# printf '\n%s\n' "--loginuid-immutable" >> /etc/audit/rules.d/98-oginuid-immutable.rules
```



## Remediation:

Configure the audit system to set the logon UIDs to be immutable by adding the following line to a **.rules** file in the **/etc/audit/rules.d/** directory

```
--loginuid-immutable
```

### Example:

```
# printf '\n%s\n' "--loginuid-immutable" >> /etc/audit/rules.d/98-oginuid-immutable.rules
```

Run the following command to merge and load the rule into active configuration:

```
# augenrules --load
```

Run the following command to check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot required to load rules\n"; fi
```

## References:

1. NIST SP 800-53 :: AU-9
2. NIST SP 800-53A :: AU-9.1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230403  
Rule ID: SV-230403r627750  
STIG ID: RHEL-08-030122  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |      | ●    | ●    |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         | ●    | ●    | ●    |

### *6.3.3.44 Ensure successful and unsuccessful modifications to the faillock file are collected (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

Successful/unsuccessful modifications to the faillock log file must generate an audit record.

#### **Rationale:**

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records.

DoD has defined the list of events for which the operating system will provide an audit record generation capability as the following:

1. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels);
2. Access actions, such as successful and unsuccessful logon attempts, privileged activities or other system-level access, starting and ending time for user access to the system, concurrent logons from different workstations, successful and unsuccessful accesses to objects, all program initiations, and all direct access to the information system;
3. All account creations, modifications, disabling, and terminations; and
4. All kernel module load, unload, and restart actions.

From "Pam\_Faillock man" pages: Note the default directory that pam\_faillock uses is usually cleared on system boot so the access will be reenabled after system reboot. If that is undesirable a different tally directory must be set with the "dir" option.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000473-GPOS-00218

## Audit:

Verify the operating system generates an audit record when successful/unsuccessful modifications to the "faillock" file occur. First, determine where the faillock tallies are stored with the following commands:

For RHEL versions 8.0 and 8.1:

```
# grep -i pam_faillock.so /etc/pam.d/system-auth  
  
auth required pam_faillock.so preauth dir=/var/log/faillock silent deny=3  
fail_interval=900 even_deny_root
```

For RHEL versions 8.2 and newer:

```
# grep dir /etc/security/faillock.conf  
  
dir=/var/log/faillock
```

Using the location of the faillock log file, check that the following calls are being audited by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
# grep -w faillock /etc/audit/audit.rules  
  
-w /var/log/faillock -p wa -k logins
```

If the command does not return a line, or the line is commented out, this is a finding.

## Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful modifications to the "faillock" file by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-w /var/log/faillock -p wa -k logins
```

The audit daemon must be restarted for the changes to take effect.

## References:

1. NIST SP 800-53 :: AU-12 a
2. NIST SP 800-53A :: AU-12.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230466  
RULE ID: SV-230466r627750  
STIG ID: RHEL-08-030590  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |                                                                                     |  |  |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         |  |  |  |

### **6.3.4 Configure auditd File Access**

Without the capability to restrict which roles and individuals can select which events are audited, unauthorized personnel may be able to prevent the auditing of critical events.

### *6.3.4.1 Ensure the audit log file directory mode is configured (Automated)*

**Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

**Description:**

The audit log directory contains audit log files.

**Rationale:**

Audit information includes all information including: audit records, audit settings and audit reports. This information is needed to successfully audit system activity. This information must be protected from unauthorized modification or deletion. If this information were to be compromised, forensic analysis and discovery of the true source of potentially malicious system activity is impossible to achieve.

## Audit:

Run the following script to verify the audit log directory is mode 0750 or more restrictive:

```
#!/usr/bin/env bash

{
    l_perm_mask="0027"
    if [ -e "/etc/audit/auditd.conf" ]; then
        l_audit_log_directory="$(dirname "$(awk -F= '/^\s*log_file\s*/{print $2}' /etc/audit/auditd.conf | xargs) ")"
        if [ -d "$l_audit_log_directory" ]; then
            l_maxperm="$(printf '%o' $(( 0777 & ~$l_perm_mask )) )"
            l_directory_mode="$(stat -Lc '%#a' "$l_audit_log_directory")"
            if [ $(( $l_directory_mode & $l_perm_mask )) -gt 0 ]; then
                echo -e "\n- Audit Result:\n  ** FAIL **\n  - Directory:
\"$l_audit_log_directory\" is mode: \"$l_directory_mode\"
mode: \"$l_maxperm\" or more restrictive)\n"
            else
                echo -e "\n- Audit Result:\n  ** PASS **\n  - Directory:
\"$l_audit_log_directory\" is mode: \"$l_directory_mode\"
mode: \"$l_maxperm\" or more restrictive)\n"
            fi
        else
            echo -e "\n- Audit Result:\n  ** FAIL **\n  - Log file directory not
set in \"/etc/audit/auditd.conf\" please set log file directory"
        fi
    else
        echo -e "\n- Audit Result:\n  ** FAIL **\n  - File:
\"/etc/audit/auditd.conf\" not found\n  - ** Verify auditd is installed **"
    fi
}
```

## Remediation:

Run the following command to configure the audit log directory to have a mode of "0750" or less permissive:

```
# chmod g-w,o-rwx "$(dirname "$(awk -F= '/^\s*log_file\s*/{print $2}' /etc/audit/auditd.conf | xargs) ")"
```

## Default Value:

750

## References:

1. NIST SP 800-53 Rev. 5: AU-3

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1083, T1083.000 | TA0007  |             |



### *6.3.4.2 Ensure audit log files mode is configured (Automated)*

**Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

**Description:**

Audit log files contain information about the system and system activity.

**Rationale:**

Access to audit records can reveal system and configuration data to attackers, potentially compromising its confidentiality.

## Audit:

Run the following script to verify audit log files are mode **0640** or more restrictive:

```
#!/usr/bin/env bash

{
    l_output="" l_output2=""
    l_perm_mask="0177"
    if [ -e "/etc/audit/auditd.conf" ]; then
        l_audit_log_directory="$(dirname "$(awk -F= '/^\s*log_file\s*/{print $2}' /etc/audit/auditd.conf | xargs) ")"
        if [ -d "$l_audit_log_directory" ]; then
            l_maxperm="$(printf '%o' $(( 0777 & ~$l_perm_mask )) )"
            while IFS= read -r -d $'\0' l_file; do
                while IFS=: read -r l_file_mode l_hr_file_mode; do
                    l_output2="$l_output2\n - File: \"$l_file\" is mode:
\"$l_file_mode\" \n          (should be mode: \"$l_maxperm\" or more
restrictive) \n"
                done <<< "$(stat -Lc '%#a:%A' "$l_file")"
                done < <(find "$l_audit_log_directory" -maxdepth 1 -type f -perm
/"$l_perm_mask" -print0)
            else
                l_output2="$l_output2\n - Log file directory not set in
\"/etc/audit/auditd.conf\" please set log file directory"
            fi
        else
            l_output2="$l_output2\n - File: \"/etc/audit/auditd.conf\" not
found.\n - ** Verify auditd is installed **"
        fi
        if [ -z "$l_output2" ]; then
            l_output="$l_output\n - All files in \"$l_audit_log_directory\" are
mode: \"$l_maxperm\" or more restrictive"
            echo -e "\n- Audit Result:\n  ** PASS **\n - * Correctly configured *
:$l_output"
        else
            echo -e "\n- Audit Result:\n  ** FAIL **\n - * Reasons for audit
failure * :$l_output2\n"
        fi
    }
}
```

## Remediation:

Run the following command to remove more permissive mode than **0640** from audit log files:

```
# [ -f /etc/audit/auditd.conf ] && find "$(dirname $(awk -F '=' '/^\s*log_file/ {print $2}' /etc/audit/auditd.conf | xargs))" -type f -perm /0137 -exec chmod u-x,g-wx,o-rwx {} +
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1083, T1083.000 | TA0007  |             |

### *6.3.4.3 Ensure audit log files owner is configured (Automated)*

**Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation
- STIG

**Description:**

Audit log files contain information about the system and system activity.

**Rationale:**

Access to audit records can reveal system and configuration data to attackers, potentially compromising its confidentiality.

## Audit:

Run the following script to verify audit log files are owned by the **root** user:

```
#!/usr/bin/env bash

{
    l_output="" l_output2=""
    if [ -e "/etc/audit/auditd.conf" ]; then
        l_audit_log_directory="$(dirname "$(awk -F= '/^\s*log_file\s*/{print $2}' /etc/audit/auditd.conf | xargs) ")"
        if [ -d "$l_audit_log_directory" ]; then
            while IFS= read -r -d $'\0' l_file; do
                l_output2="$l_output2\n - File: \"$l_file\" is owned by user: \n$(stat -Lc '%U' "$l_file")\n\n (should be owned by user: \"root\")\n"
            done < <(find "$l_audit_log_directory" -maxdepth 1 -type f ! -user root -print0)
            else
                l_output2="$l_output2\n - Log file directory not set in \n/etc/audit/auditd.conf\n please set log file directory"
            fi
        else
            l_output2="$l_output2\n - File: \n/etc/audit/auditd.conf\n not found.\n - ** Verify auditd is installed **"
            fi
        if [ -z "$l_output2" ]; then
            l_output="$l_output\n - All files in \"$l_audit_log_directory\" are owned by user: \"root\"\n"
            echo -e "\n- Audit Result:\n ** PASS **\n - * Correctly configured * :$l_output"
        else
            echo -e "\n- Audit Result:\n ** FAIL **\n - * Reasons for audit failure * :$l_output2\n"
            fi
    }
}
```

## Remediation:

Run the following command to configure the audit log files to be owned by the **root** user:

```
# [ -f /etc/audit/auditd.conf ] && find "$(dirname $(awk -F= '/^\s*log_file/ {print $2}' /etc/audit/auditd.conf | xargs) )" -type f ! -user root -exec chown root {} +
```

## References:

1. NIST SP 800-53 :: CM-7
2. NIST SP 800-53A :: CM-7.1 (ii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230397  
Rule ID: SV-230397r627750  
STIG ID: RHEL-08-030080  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1083, T1083.000 | TA0007  | M1022       |

#### *6.3.4.4 Ensure audit log files group owner is configured (Automated)*

**Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

**Description:**

Audit log files contain information about the system and system activity.

**Rationale:**

Access to audit records can reveal system and configuration data to attackers, potentially compromising its confidentiality.

## Audit:

Run the following script to verify:

- **log\_group** parameter is set to either **adm** or **root** in **/etc/audit/auditd.conf**
- audit log files are group owned by the group "root" or "adm"

```
#!/usr/bin/env bash

{
    l_output="" l_output2=""
    if [ -e "/etc/audit/auditd.conf" ]; then
        l_audit_log_directory="$(dirname "$(awk -F= '/^\s*log_file\s*/{print $2}' /etc/audit/auditd.conf | xargs) ")"
        l_audit_log_group="$(awk -F= '/^\s*log_group\s*/{print $2}' /etc/audit/auditd.conf | xargs) "
        if grep -Pq -- '^\h*(root|adm)\h*$' <<< "$l_audit_log_group"; then
            l_output="$l_output\n - Log file group correctly set to: \"$l_audit_log_group\" in \"/etc/audit/auditd.conf\""
        else
            l_output2="$l_output2\n - Log file group is set to: \"$l_audit_log_group\" in \"/etc/audit/auditd.conf\" (should be set to group: \"root or adm\")\n"
        fi
        if [ -d "$l_audit_log_directory" ]; then
            while IFS= read -r -d $'\0' l_file; do
                l_output2="$l_output2\n - File: \"$l_file\" is group owned by group: \"$(stat -Lc '%G' "$l_file")\" (should be group owned by group: \"root or adm\")\n"
            done <<(find "$l_audit_log_directory" -maxdepth 1 -type f \( ! -group root -a ! -group adm \) -print0)
        else
            l_output2="$l_output2\n - Log file directory not set in \"/etc/audit/auditd.conf\" please set log file directory"
        fi
        else
            l_output2="$l_output2\n - File: \"/etc/audit/auditd.conf\" not found.\n - ** Verify auditd is installed **"
        fi
        if [ -z "$l_output2" ]; then
            l_output="$l_output\n - All files in \"$l_audit_log_directory\" are group owned by group: \"root or adm\"\n"
            echo -e "\n- Audit Result:\n ** PASS **\n - * Correctly configured * :$l_output"
        else
            echo -e "\n- Audit Result:\n ** FAIL **\n - * Reasons for audit failure * :$l_output2\n"
            [ -n "$l_output" ] && echo -e " - * Correctly configured * :$l_output\n"
        fi
    fi
}
```



## Remediation:

Run the following command to configure the audit log files to be owned by **adm** group:

```
# find $(dirname $(awk -F"=" ' /^\s*log_file\s*=\s*/ {print $2}'  
/etc/audit/auditd.conf | xargs)) -type f \( ! -group adm -a ! -group root \)  
-exec chgrp adm {} +
```

Run the following command to configure the audit log files to be owned by the **adm** group:

```
# chgrp adm /var/log/audit/
```

Run the following command to set the **log\_group** parameter in the audit configuration file to **log\_group = adm**:

```
# sed -ri 's/^\s*#\?\s*log_group\s*=\s*\S+(\s*#.*)?.*$/log_group = adm\1/'  
/etc/audit/auditd.conf
```

Run the following command to restart the audit daemon to reload the configuration file:

```
# systemctl restart auditd
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 Protect Information through Access Control Lists</b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1083, T1083.000 | TA0007  |             |

### *6.3.4.5 Ensure audit configuration files mode is configured (Automated)*

**Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation
- STIG

**Description:**

Audit configuration files control auditd and what events are audited.

**Rationale:**

Access to the audit configuration files could allow unauthorized personnel to prevent the auditing of critical events.

Misconfigured audit configuration files may prevent the auditing of critical events or impact the system's performance by overwhelming the audit log. Misconfiguration of the audit configuration files may also make it more difficult to establish and investigate events relating to an incident.

## Audit:

Run the following script to verify that the audit configuration files are mode **0640** or more restrictive:

```
#!/usr/bin/env bash

{
  l_output="" l_output2="" l_perm_mask="0137"
  l_maxperm="$( printf '%o' $(( 0777 & ~$l_perm_mask )) )"
  while IFS= read -r -d $'\0' l_fname; do
    l_mode=$(stat -Lc '%#a' "$l_fname")
    if [ $(( "$l_mode" & "$l_perm_mask" )) -gt 0 ]; then
      l_output2="$l_output2\n - file: \"$l_fname\" is mode: \"$l_mode\"
(should be mode: \"$l_maxperm\" or more restrictive)"
    fi
    done < <(find /etc/audit/ -type f \( -name "*.conf" -o -name '*.rules' \)
-print0)
    if [ -z "$l_output2" ]; then
      echo -e "\n- Audit Result:\n  ** PASS **\n - All audit configuration
files are mode: \"$l_maxperm\" or more restrictive"
    else
      echo -e "\n- Audit Result:\n  ** FAIL **\n$l_output2"
    fi
  }
}
```

## Remediation:

Run the following command to remove more permissive mode than 0640 from the audit configuration files:

```
# find /etc/audit/ -type f \( -name '*.conf' -o -name '*.rules' \) -exec
chmod u-x,g-wx,o-rwx {} +
```

## References:

1. NIST SP 800-53 :: AU-12 b
2. NIST SP 800-53A :: AU-12.1 (iii)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230471  
Rule ID: SV-230471r627750  
STIG ID: RHEL-08-030610  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1083, T1083.000 | TA0007  |             |

### 6.3.4.6 Ensure audit configuration files owner is configured (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

#### Description:

Audit configuration files control auditd and what events are audited.

#### Rationale:

Access to the audit configuration files could allow unauthorized personnel to prevent the auditing of critical events.

Misconfigured audit configuration files may prevent the auditing of critical events or impact the system's performance by overwhelming the audit log. Misconfiguration of the audit configuration files may also make it more difficult to establish and investigate events relating to an incident.

#### Audit:

Run the following command to verify that the audit configuration files have mode 640 or more restrictive and are owned by the root user and root group:

```
# find /etc/audit/ -type f \( -name '*.conf' -o -name '*.rules' \) ! -user root
```

Nothing should be returned

#### Remediation:

Run the following command to change ownership to **root** user:

```
# find /etc/audit/ -type f \( -name '*.conf' -o -name '*.rules' \) ! -user root -exec chown root {} +
```

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1083, T1083.000 | TA0007  |             |

### 6.3.4.7 Ensure audit configuration files group owner is configured (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

#### Description:

Audit configuration files control auditd and what events are audited.

#### Rationale:

Access to the audit configuration files could allow unauthorized personnel to prevent the auditing of critical events.

Misconfigured audit configuration files may prevent the auditing of critical events or impact the system's performance by overwhelming the audit log. Misconfiguration of the audit configuration files may also make it more difficult to establish and investigate events relating to an incident.

#### Audit:

Run the following command to verify that the audit configuration files are owned by the group **root**:

```
# find /etc/audit/ -type f \( -name '*.conf' -o -name '*.rules' \) ! -group root
```

Nothing should be returned

#### Remediation:

Run the following command to change group to **root**:

```
# find /etc/audit/ -type f \( -name '*.conf' -o -name '*.rules' \) ! -group root -exec chgrp root {} +
```

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1083, T1083.000 | TA0007  |             |



#### *6.3.4.8 Ensure audit tools mode is configured (Automated)*

**Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

**Description:**

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

**Rationale:**

Protecting audit information includes identifying and protecting the tools used to view and manipulate log data. Protecting audit tools is necessary to prevent unauthorized operation on audit information.

## Audit:

Run the following script to verify the audit tools are mode **0755** or more restrictive:

```
#!/usr/bin/env bash

{
    l_output="" l_output2="" l_perm_mask="0022"
    l_maxperm="$( printf '%o' $(( 0777 & ~$l_perm_mask )) )"
    a_audit_tools=("/sbin/auditctl" "/sbin/aureport" "/sbin/ausearch"
"/sbin/autrace" "/sbin/auditd" "/sbin/augenrules")
    for l_audit_tool in "${a_audit_tools[@]"; do
        l_mode="$(stat -Lc '%a' "$l_audit_tool")"
        if [ $(( "$l_mode" & "$l_perm_mask" )) -gt 0 ]; then
            l_output2="$l_output2\n - Audit tool \"$l_audit_tool\" is mode:
\"$l_mode\" and should be mode: \"$l_maxperm\" or more restrictive"
        else
            l_output="$l_output\n - Audit tool \"$l_audit_tool\" is correctly
configured to mode: \"$l_mode\""
        fi
    done
    if [ -z "$l_output2" ]; then
        echo -e "\n- Audit Result:\n  ** PASS **\n - * Correctly configured *
:$l_output"
    else
        echo -e "\n- Audit Result:\n  ** FAIL **\n - * Reasons for audit
failure * :$l_output2\n"
        [ -n "$l_output" ] && echo -e "\n - * Correctly configured *
:\n$l_output\n"
    fi
    unset a_audit_tools
}
```

## Remediation:

Run the following command to remove more permissive mode from the audit tools:

```
# chmod go-w /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace
/sbin/auditd /sbin/augenrules
```

## References:

1. NIST SP 800-53 Rev. 5: AU-3

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1083, T1083.000 | TA0007  |             |

### 6.3.4.9 Ensure audit tools owner is configured (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

#### Description:

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

#### Rationale:

Protecting audit information includes identifying and protecting the tools used to view and manipulate log data. Protecting audit tools is necessary to prevent unauthorized operation on audit information.

#### Audit:

Run the following command to verify the audit tools are owned by the **root** user:

```
# stat -Lc "%n %U" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /sbin/auditd /sbin/auditd /sbin/auditd | awk '$2 != "root" {print}'
```

Nothing should be returned

#### Remediation:

Run the following command to change the owner of the audit tools to the **root** user:

```
# chown root /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /sbin/auditd /sbin/auditd /sbin/auditd
```

#### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 Protect Information through Access Control Lists</b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1083, T1083.000 | TA0007  |             |

### 6.3.4.10 Ensure audit tools group owner is configured (Automated)

#### Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

#### Description:

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

#### Rationale:

Protecting audit information includes identifying and protecting the tools used to view and manipulate log data. Protecting audit tools is necessary to prevent unauthorized operation on audit information.

#### Audit:

Run the following command to verify the audit tools are owned by the group **root**

```
# stat -Lc "%n %G" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /sbin/auditd /sbin/augenrules | awk '$2 != "root" {print}'
```

Nothing should be returned

#### Remediation:

Run the following command to change group ownership to the group **root**:

```
# chgrp root /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /sbin/auditd /sbin/augenrules
```

#### References:

1. NIST SP 800-53 Rev. 5: AU-3

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1070, T1070.002, T1083, T1083.000 | TA0007  | M1022       |

### 6.3.4.11 *Ensure the audit logs are group-owned by root* (Automated)

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system's audit logs must be group-owned by root to prevent unauthorized read access.

#### **Rationale:**

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit the operating system's activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

#### **Audit:**

Verify the audit logs are group-owned by "root". First determine where the audit logs are stored with the following command:

```
# grep -iw log_file /etc/audit/auditd.conf  
log_file = /var/log/audit/audit.log
```

Using the location of the audit log file, determine if the audit log is group-owned by "root" using the following command:

```
ls -al /var/log/audit/audit.log  
rw----- 2 root root 23 Jun 11 11:56 /var/log/audit/audit.log
```

If the audit log is not group-owned by "root", this is a finding.



Remediation:

Configure the audit log to be owned by root by configuring the log group in the /etc/audit/auditd.conf file:

```
log_group = root
```

Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230398  
Rule ID: SV-230398r627750  
STIG ID: RHEL-08-030090  
Severity: CAT II

CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1        | IG 2        | IG 3        |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-------------|-------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        | <div></div> | <div></div> | <div></div> |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | <div></div> | <div></div> | <div></div> |

### 6.3.4.12 *Ensure audit tools are mode 0755 or more restrictive (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system's audit tools must have a mode of 0755 or less permissive.

#### **Rationale:**

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

RHEL 8 systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools, and the corresponding rights the user enjoys, to make access decisions regarding the access to audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

#### **Audit:**

Verify the audit tools are protected from unauthorized access, deletion, or modification by checking the permissive mode.

Check the octal permission of each audit tool by running the following command:

```
# stat -c "%a %n" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace  
/sbin/auditd /sbin/rsyslogd /sbin/augenrules  
  
755 /sbin/auditctl  
755 /sbin/aureport  
755 /sbin/ausearch  
750 /sbin/autrace  
755 /sbin/auditd  
755 /sbin/rsyslogd  
755 /sbin/augenrules
```

If any of the audit tools has a mode more permissive than "0755", this is a finding.

#### **Remediation:**

Configure the audit tools to be protected from unauthorized access by setting the correct permissive mode using the following command:

```
# chmod 0755 [audit_tool]
```

Replace "[audit\_tool]" with the audit tool that does not have the correct permissive mode.

## References:

1. NIST SP 800-53 :: AU-9
2. NIST SP 800-53A :: AU-9.1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230472  
Rule ID: SV-230472r627750  
STIG ID: RHEL-08-030620  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |    |    |    |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### 6.3.4.13 *Ensure the audit tools are owned by root (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system's audit tools must be owned by root.

#### **Rationale:**

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

RHEL 8 systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools, and the corresponding rights the user enjoys, to make access decisions regarding the access to audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Satisfies: SRG-OS-000256-GPOS-00097, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099

#### **Audit:**

Verify the audit tools are owned by "root" to prevent any unauthorized access, deletion, or modification.

Check the owner of each audit tool by running the following command:

```
# stat -c "%U %n" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace  
/sbin/auditd /sbin/rsyslogd /sbin/augenrules  
  
root /sbin/auditctl  
root /sbin/aureport  
root /sbin/ausearch  
root /sbin/autrace  
root /sbin/auditd  
root /sbin/rsyslogd  
root /sbin/augenrules
```

If any of the audit tools are not owned by "root", this is a finding.

#### **Remediation:**

Configure the audit tools to be owned by "root", by running the following command:

```
# chown root [audit_tool]
```

Replace "[audit\_tool]" with each audit tool not owned by "root".

## References:

1. NIST SP 800-53 :: AU-9
2. NIST SP 800-53A :: AU-9.1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230473  
Rule ID: SV-230473r744008  
STIG ID: RHEL-08-030630  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |    |    |    |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### 6.3.4.14 Ensure audit tools are group owned by root (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system's audit tools must be group-owned by root.

#### Rationale:

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

RHEL 8 systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools, and the corresponding rights the user enjoys, to make access decisions regarding the access to audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Satisfies: SRG-OS-000256-GPOS-00097, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099

#### Audit:

Verify the audit tools are group-owned by "root" to prevent any unauthorized access, deletion, or modification.

Check the owner of each audit tool by running the following commands:

```
# stat -c "%G %n" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace
/sbin/auditd /sbin/rsyslogd /sbin/augenrules

root /sbin/auditctl
root /sbin/aureport
root /sbin/ausearch
root /sbin/autrace
root /sbin/auditd
root /sbin/rsyslogd
root /sbin/augenrules
```

If any of the audit tools are not group-owned by "root", this is a finding.

#### Remediation:

Configure the audit tools to be group-owned by "root", by running the following command:

```
# chgrp root [audit_tool]
```

Replace "[audit\_tool]" with each audit tool not group-owned by "root".

## References:

1. NIST SP 800-53 :: AU-9
2. NIST SP 800-53A :: AU-9.1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230474  
Rule ID: SV-230474r627750  
STIG ID: RHEL-08-030640  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |    |    |    |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### 6.3.4.15 Ensure the audit log file directories are mode 0700 or more restrictive (Automated)

#### Profile Applicability:

- STIG

#### Description:

The audit log directory must have a mode of 0700 or less permissive to prevent unauthorized read access.

#### Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit system activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

#### Audit:

Verify the audit log directories have a mode of "0700" or less permissive by first determining where the audit logs are stored with the following command:

```
# grep -iw log_file /etc/audit/auditd.conf  
  
log_file = /var/log/audit/audit.log
```

Using the location of the audit log, determine the directory where the audit logs are stored (ex: "/var/log/audit"). Run the following command to determine the permissions for the audit log folder:

```
# stat -c "%a %n" /var/log/audit  
  
700 /var/log/audit
```

If the audit log directory has a mode more permissive than "0700", this is a finding.

#### Remediation:

Configure the audit log directory to be protected from unauthorized read access by setting the correct permissive mode with the following command:

```
# chmod 0700 [audit_log_directory]
```

Replace "[audit\_log\_directory]" to the correct audit log directory path, by default this location is "/var/log/audit".



## References:

1. NIST SP 800-53 :: AU-9
2. NIST SP 800-53A :: AU-9.1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230401  
Rule ID: SV-230401r627750  
STIG ID: RHEL-08-030120  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |    |    |    |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### 6.3.4.16 *Ensure the audit log file directory is owned by root (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The audit log directory must be owned by root to prevent unauthorized read access.

#### **Rationale:**

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit the operating system's activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

#### **Audit:**

Verify the audit log directory is owned by "root" to prevent unauthorized read access. Determine where the audit logs are stored with the following command:

```
# grep -iw log_file /etc/audit/auditd.conf  
  
log_file = /var/log/audit/audit.log
```

Determine the owner of the audit log directory by using the output of the above command (ex: "/var/log/audit/"). Run the following command with the correct audit log directory path:

```
# ls -ld /var/log/audit  
  
drw----- 2 root root 23 Jun 11 11:56 /var/log/audit
```

If the audit log directory is not owned by "root", this is a finding.

#### **Remediation:**

Configure the audit log to be protected from unauthorized read access, by setting the correct owner as "root" with the following command:

```
# chown root [audit_log_directory]
```

Replace "[audit\_log\_directory]" with the correct audit log directory path, by default this location is usually "/var/log/audit".

## References:

1. NIST SP 800-53 :: AU-9
2. NIST SP 800-53A :: AU-9.1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230399  
Rule ID: SV-230399r627750  
STIG ID: RHEL-08-030100  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |    |    |    |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### 6.3.4.17 Ensure audit log files group owner is root (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system's audit log directory must be group-owned by root to prevent unauthorized read access.

#### Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit the operating system's activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

#### Audit:

Verify the audit log directory is group-owned by "root" to prevent unauthorized read access.

Determine where the audit logs are stored with the following command:

```
# grep -iw log_file /etc/audit/auditd.conf

log_file = /var/log/audit/audit.log
```

Determine the group owner of the audit log directory by using the output of the above command (ex: "/var/log/audit/"). Run the following command with the correct audit log directory path:

```
# ls -ld /var/log/audit

drw----- 2 root root 23 Jun 11 11:56 /var/log/audit
^^^
```

If the audit log directory is not group-owned by "root", this is a finding.

#### Remediation:

Configure the audit log to be protected from unauthorized read access by setting the correct group-owner as "root" with the following command:

```
# chgrp root [audit_log_directory]
```

Replace "[audit\_log\_directory]" with the correct audit log directory path, by default this location is usually "/var/log/audit".

## References:

1. NIST SP 800-53 :: AU-9
2. NIST SP 800-53A :: AU-9.1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230400  
Rule ID: SV-230400r627750  
STIG ID: RHEL-08-030110  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |    |    |    |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### 6.3.4.18 Ensure audit log files are mode 0600 or more restrictive (Automated)

#### Profile Applicability:

- STIG

#### Description:

The operating system's audit logs must have a mode of 0600 or less permissive to prevent unauthorized read access.

#### Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029, SRG-OS-000206-GPOS-00084

#### Audit:

Verify the audit logs have a mode of "0600" or less permissive.

First, determine where the audit logs are stored with the following command:

```
# grep -iw log_file /etc/audit/auditd.conf  
log_file = /var/log/audit/audit.log
```

Using the location of the audit log file, check if the audit log has a mode of "0600" or less permissive with the following command:

```
# stat -c "%a %n" /var/log/audit/audit.log  
600 /var/log/audit/audit.log
```

If the audit log has a mode more permissive than "0600", this is a finding.

## Remediation:

Configure the audit log to be protected from unauthorized read access by configuring the log group in the /etc/audit/auditd.conf file:

```
# chmod 0600 /var/log/audit/audit.log
```

## References:

1. NIST SP 800-53 Revision 5 :: AU-9 a
2. NIST SP 800-53A :: AU-9.1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230396  
Rule ID: SV-230396r902733  
STIG ID: RHEL-08-030070  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## 7 System Maintenance

Recommendations in this section are intended as maintenance and are intended to be checked on a frequent basis to ensure system stability. Many recommendations do not have quick remediations and require investigation into the cause and best fix available and may indicate an attempted breach of system security.



## 7.1 System File Permissions

This section provides guidance on securing aspects of system files and directories.

### 7.1.1 Ensure permissions on /etc/passwd are configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The `/etc/passwd` file contains user account information that is used by many system utilities and therefore must be readable for these utilities to operate.

#### Rationale:

It is critical to ensure that the `/etc/passwd` file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

#### Audit:

Run the following command to verify `/etc/passwd` is mode 644 or more restrictive, `Uid` is `0/root` and `Gid` is `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/passwd
Access: (0644/-rw-r--r--)  Uid: ( 0/ root) Gid: ( 0/ root)
```

#### Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/passwd`:

```
# chmod u-x,go-wx /etc/passwd
# chown root:root /etc/passwd
```

#### Default Value:

Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)

#### References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1003, T1003.008, T1222, T1222.002 | TA0005  | M1022       |

## 7.1.2 Ensure permissions on /etc/passwd- are configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The `/etc/passwd-` file contains backup user account information.

### Rationale:

It is critical to ensure that the `/etc/passwd-` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### Audit:

Run the following command to verify `/etc/passwd-` is mode 644 or more restrictive, `Uid` is `0/root` and `Gid` is `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: { %g/ %G)' /etc/passwd-  
Access: (0644/-rw-r--r--)  Uid: ( 0/ root) Gid: { 0/ root)
```

### Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/passwd-`:

```
# chmod u-x,go-wx /etc/passwd-  
# chown root:root /etc/passwd-
```

### Default Value:

Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: { 0/ root)

### References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1003, T1003.008, T1222, T1222.002 | TA0005  | M1022       |

### 7.1.3 Ensure permissions on /etc/group are configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The `/etc/group` file contains a list of all the valid groups defined in the system. The command below allows read/write access for root and read access for everyone else.

#### Rationale:

The `/etc/group` file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.

#### Audit:

Run the following command to verify `/etc/group` is mode 644 or more restrictive, `Uid` is `0/root` and `Gid` is `0/root`:

```
# stat -Lc 'Access: (%a/%A)  Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/group
Access: (0644/-rw-r--r--)  Uid: ( 0/ root) Gid: ( 0/ root)
```

#### Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/group`:

```
# chmod u-x,go-wx /etc/group
# chown root:root /etc/group
```

#### Default Value:

Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)

#### References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1003, T1003.008, T1222, T1222.002 | TA0005  | M1022       |

## 7.1.4 Ensure permissions on /etc/group- are configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The `/etc/group-` file contains a backup list of all the valid groups defined in the system.

### Rationale:

It is critical to ensure that the `/etc/group-` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### Audit:

Run the following command to verify `/etc/group-` is mode 644 or more restrictive, `Uid` is `0/root` and `Gid` is `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/group-  
Access: (0644/-rw-r--r--)  Uid: ( 0/ root) Gid: ( 0/ root)
```

### Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/group-`:

```
# chmod u-x,go-wx /etc/group-  
# chown root:root /etc/group-
```

### Default Value:

Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)

### References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2



## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1003, T1003.008, T1222, T1222.002 | TA0005  | M1022       |

## 7.1.5 Ensure permissions on /etc/shadow are configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The `/etc/shadow` file is used to store the information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

### Rationale:

If attackers can gain read access to the `/etc/shadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/shadow` file (such as expiration) could also be useful to subvert the user accounts.

### Audit:

Run the following command to verify `/etc/shadow` is mode 000, Uid is 0/root and Gid is 0/root:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: ( %g/ %G) ' /etc/shadow
Access: (0/-----)  Uid: ( 0/ root) Gid: ( 0/ root)
```

### Remediation:

Run the following commands to set mode, owner, and group on `/etc/shadow`:

```
# chown root:root /etc/shadow
# chmod 0000 /etc/shadow
```

### Default Value:

Access: (0/-----) Uid: ( 0/ root) Gid: ( 0/ root)

### References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1003, T1003.008, T1222, T1222.002 | TA0005  | M1022       |

## 7.1.6 Ensure permissions on /etc/shadow- are configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The `/etc/shadow-` file is used to store backup information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

### Rationale:

It is critical to ensure that the `/etc/shadow-` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### Audit:

Run the following command to verify `/etc/shadow-` is mode 000, `Uid` is `0/root` and `Gid` is `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/shadow-  
Access: (0/-----)  Uid: ( 0/ root) Gid: ( 0/ root)
```

### Remediation:

Run the following commands to set mode, owner, and group on `/etc/shadow-`:

```
# chown root:root /etc/shadow-  
# chmod 0000 /etc/shadow-
```

### Default Value:

Access: (0/-----) Uid: ( 0/ root) Gid: ( 0/ root)

### References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1003, T1003.008, T1222, T1222.002 | TA0005  | M1022       |

## 7.1.7 Ensure permissions on /etc/gshadow are configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The `/etc/gshadow` file is used to store the information about groups that is critical to the security of those accounts, such as the hashed password and other security information.

### Rationale:

If attackers can gain read access to the `/etc/gshadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/gshadow` file (such as group administrators) could also be useful to subvert the group.

### Audit:

Run the following command to verify `/etc/gshadow` is mode 000, `Uid` is `0/root` and `Gid` is `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/gshadow
Access: (0/-----)  Uid: ( 0/ root) Gid: ( 0/ root)
```

### Remediation:

Run the following commands to set mode, owner, and group on `/etc/gshadow`:

```
# chown root:root /etc/gshadow
# chmod 0000 /etc/gshadow
```

### Default Value:

Access: (0/-----) Uid: ( 0/ root) Gid: ( 0/ root)

### References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |
| v7               | <b>16.4 <u>Encrypt or Hash all Authentication Credentials</u></b><br>Encrypt or hash with a salt all authentication credentials when stored.                                                                                                                   |                                                                                     |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1003, T1003.008, T1222, T1222.002 | TA0005  | M1022       |

## 7.1.8 Ensure permissions on /etc/gshadow- are configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The `/etc/gshadow-` file is used to store backup information about groups that is critical to the security of those accounts, such as the hashed password and other security information.

### Rationale:

It is critical to ensure that the `/etc/gshadow-` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### Audit:

Run the following command to verify `/etc/gshadow-` is mode 000, Uid is 0/root and Gid is 0/root:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/gshadow-  
Access: (0/-----)  Uid: ( 0/ root) Gid: ( 0/ root)
```

### Remediation:

Run the following commands to set mode, owner, and group on `/etc/gshadow-`:

```
# chown root:root /etc/gshadow-  
# chmod 0000 /etc/gshadow-
```

### Default Value:

Access: (0/-----) Uid: ( 0/ root) Gid: ( 0/ root)

### References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2



## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |
| v7               | <b>16.4 <u>Encrypt or Hash all Authentication Credentials</u></b><br>Encrypt or hash with a salt all authentication credentials when stored.                                                                                                                   |                                                                                     |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1003, T1003.008, T1222, T1222.002 | TA0005  | M1022       |

## 7.1.9 Ensure permissions on /etc/shells are configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

`/etc/shells` is a text file which contains the full pathnames of valid login shells. This file is consulted by `chsh` and available to be queried by other programs.

### Rationale:

It is critical to ensure that the `/etc/shells` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### Audit:

Run the following command to verify `/etc/shells` is mode 644 or more restrictive, `Uid` is `0/root` and `Gid` is `0/root`:

```
# stat -Lc 'Access: (%#a/%A)  Uid: ( %u/ %U) Gid: ( %g/ %G)' /etc/shells
Access: (0644/-rw-r--r--)  Uid: ( 0/ root) Gid: ( 0/ root)
```

### Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/shells`:

```
# chmod u-x,go-wx /etc/shells
# chown root:root /etc/shells
```

### Default Value:

Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)

### References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1003, T1003.008, T1222, T1222.002 | TA0005  | M1022       |

## 7.1.10 Ensure permissions on /etc/security/opasswd are configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

`/etc/security/opasswd` and its backup `/etc/security/opasswd.old` hold user's previous passwords if `pam_unix` or `pam_pwhistory` is in use on the system

### Rationale:

It is critical to ensure that `/etc/security/opasswd` is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### Audit:

Run the following commands to verify `/etc/security/opasswd` and `/etc/security/opasswd.old` are mode 600 or more restrictive, `Uid` is `0/root` and `Gid` is `0/root` if they exist:

```
# [ -e "/etc/security/opasswd" ] && stat -Lc '%n Access: (%#a/%A)  Uid: (
%u/ %U)  Gid: ( %g/ %G)' /etc/security/opasswd

/etc/security/opasswd Access: (0600/-rw-----)  Uid: ( 0/ root) Gid: ( 0/
root)
-OR-
Nothing is returned
# [ -e "/etc/security/opasswd.old" ] && stat -Lc '%n Access: (%#a/%A)  Uid:
( %u/ %U)  Gid: ( %g/ %G)' /etc/security/opasswd.old

/etc/security/opasswd.old Access: (0600/-rw-----)  Uid: ( 0/ root) Gid: (
0/ root)
-OR-
Nothing is returned
```

## Remediation:

Run the following commands to remove excess permissions, set owner, and set group on `/etc/security/opasswd` and `/etc/security/opasswd.old` if they exist:

```
# [ -e "/etc/security/opasswd" ] && chmod u-x,go-rwx /etc/security/opasswd
# [ -e "/etc/security/opasswd" ] && chown root:root /etc/security/opasswd
# [ -e "/etc/security/opasswd.old" ] && chmod u-x,go-rwx /etc/security/opasswd.old
# [ -e "/etc/security/opasswd.old" ] && chown root:root /etc/security/opasswd.old
```

## Default Value:

`/etc/security/opasswd` Access: (0600/-rw-----) Uid: ( 0/ root) Gid: ( 0/ root)

## References:

1. NIST SP 800-53 Rev. 5: AC-3, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 Protect Information through Access Control Lists</b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques        | Tactics | Mitigations |
|------------------------------------|---------|-------------|
| T1003, T1003.008, T1222, T1222.002 | TA0005  | M1022       |

### *7.1.11 Ensure world writable files and directories are secured (Automated)*

**Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation
- STIG

**Description:**

World writable files are the least secure. Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity. See the `chmod(2)` man page for more information.

Setting the sticky bit on world writable directories prevents users from deleting or renaming files in that directory that are not owned by them.

**Rationale:**

Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.

This feature prevents the ability to delete or rename files in world writable directories (such as `/tmp`) that are owned by another user.

**Audit:**

Run the following script to verify:

- No world writable files exist
- No world writable directories without the sticky bit exist

```
#!/usr/bin/env bash

{
    l_output="" l_output2=""
    l_smask='01000'
    a_file=(); a_dir=() # Initialize arrays
    a_path=(! -path "/run/user/*" -a ! -path "/proc/*" -a ! -path
"/containerd/*" -a ! -path "*/kubelet/pods/*" -a ! -path
"/kubelet/plugins/*" -a ! -path "/sys/*" -a ! -path "/snap/*")
    while IFS= read -r l_mount; do
        while IFS= read -r -d $'\0' l_file; do
            if [ -e "$l_file" ]; then
                [ -f "$l_file" ] && a_file+=("$l_file") # Add WR files
                if [ -d "$l_file" ]; then # Add directories w/o sticky bit
                    l_mode="$(stat -Lc '%#a' "$l_file")"
                    [ ! $(( $l_mode & $l_smask )) -gt 0 ] && a_dir+=("$l_file")
                fi
            fi
        done <<(find "$l_mount" -xdev \( "${a_path[@]}" \) \( -type f -o -type
d \) -perm -0002 -print0 2> /dev/null)
        done <<(findmnt -Dkerno fstype,target | awk '($1 !~
/^\\s*(nfs|proc|smb|vfat|iso9660|efivarfs|selinuxfs)/ && $2 !~
/^(\\/run\\/user\\/|\\/tmp\\/|\\/var\\/tmp\\/){print $2}')
        if ! (( ${#a_file[@]} > 0 )); then
            l_output="$l_output\n - No world writable files exist on the local
filesystem."
        else
            l_output2="$l_output2\n - There are \"$(printf '%s' "${#a_file[@]}")\"
World writable files on the system.\n - The following is a list of World
writable files:\n$(printf '%s\n' "${a_file[@]}")\n - end of list\n"
            fi
            if ! (( ${#a_dir[@]} > 0 )); then
                l_output="$l_output\n - Sticky bit is set on world writable
directories on the local filesystem."
            else
                l_output2="$l_output2\n - There are \"$(printf '%s' "${#a_dir[@]}")\"
World writable directories without the sticky bit on the system.\n - The
following is a list of World writable directories without the sticky
bit:\n$(printf '%s\n' "${a_dir[@]}")\n - end of list\n"
                fi
            unset a_path; unset a_arr; unset a_file; unset a_dir # Remove arrays
            # If l_output2 is empty, we pass
            if [ -z "$l_output2" ]; then
                echo -e "\n- Audit Result:\n ** PASS **\n - * Correctly configured *
:\n$l_output\n"
            else
                echo -e "\n- Audit Result:\n ** FAIL **\n - * Reasons for audit
failure * :\n$l_output2"
                [ -n "$l_output" ] && echo -e "- * Correctly configured *
:\n$l_output\n"
            fi
        }
}
```

**Note:** On systems with a large number of files and/or directories, this audit may be a long running process

## Remediation:

- World Writable Files:
  - It is recommended that write access is removed from **other** with the command ( **chmod o-w <filename>** ), but always consult relevant vendor documentation to avoid breaking any application dependencies on a given file.
- World Writable Directories:
  - Set the sticky bit on all world writable directories with the command ( **chmod a+t <directory\_name>** )

Run the following script to:

- Remove other write permission from any world writable files
- Add the sticky bit to all world writable directories

```
#!/usr/bin/env bash

{
    l_smask='01000'
    a_file=(); a_dir=() # Initialize arrays
    a_path=(! -path "/run/user/*" -a ! -path "/proc/*" -a ! -path
"/containerd/*" -a ! -path "*/kubelet/pods/*" -a ! -path
"/kubelet/plugins/*" -a ! -path "/sys/*" -a ! -path "/snap/*")
    while IFS= read -r l_mount; do
        while IFS= read -r -d $'\0' l_file; do
            if [ -e "$l_file" ]; then
                l_mode="$(stat -Lc '%#a' "$l_file")"
                if [ -f "$l_file" ]; then # Remove excess permissions from WW
files
                    echo -e " - File: \"$l_file\" is mode: \"$l_mode\" \n -
removing write permission on \"$l_file\" from \"other\""
                    chmod o-w "$l_file"
                fi
                if [ -d "$l_file" ]; then # Add sticky bit
                    if [ ! $(( $l_mode & $l_smask )) -gt 0 ]; then
                        echo -e " - Directory: \"$l_file\" is mode: \"$l_mode\" and
doesn't have the sticky bit set \n - Adding the sticky bit"
                        chmod a+t "$l_file"
                    fi
                fi
            fi
        done <<(find "$l_mount" -xdev \( "${a_path[@]}" \) \( -type f -o -type
d \) -perm -0002 -print0 2> /dev/null)
        done <<(findmnt -Dkerno fstype,target | awk '($1 !~
/^s*(nfs|proc|smb|vfat|iso9660|efivarfs|selinuxfs)/ && $2 !~
/^(\/run\/user\/|\/tmp\/var\/tmp)/){print $2}')
    }
}
```



## References:

1. NIST SP 800-53 Rev. 5: AC-3. MP-2
2. NIST SP 800-53A :: SC-4.1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230243  
Rule ID: SV-230243r792857  
STIG ID: RHEL-08-8-010190  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |    |    |    |
| v7               | <b>14.6 Protect Information through Access Control Lists</b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics        | Mitigations  |
|-----------------------------|----------------|--------------|
| T1222, T1222.002, T1548     | TA0004, TA0005 | M1022, M1028 |

### *7.1.12 Ensure no files or directories without an owner and a group exist (Automated)*

**Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation
- STIG

**Description:**

Administrators may delete users or groups from the system and neglect to remove all files and/or directories owned by those users or groups.

**Rationale:**

A new user or group who is assigned a deleted user's user ID or group ID may then end up "owning" a deleted user or group's files, and thus have more access on the system than was intended.

**Audit:**

Run the following script to verify no unowned or ungrouped files or directories exist:

```
#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_nouser=(); a_nogroup=() # Initialize arrays
    a_path=(! -path "/run/user/*" -a ! -path "/proc/*" -a ! -path
"/containerd/*" -a ! -path "*/kubelet/pods/*" -a ! -path
"/kubelet/plugins/*" -a ! -path "/sys/fs/cgroup/memory/*" -a ! -path
"/var/*/private/*")
    while IFS= read -r l_mount; do
        while IFS= read -r -d $'\0' l_file; do
            if [ -e "$l_file" ]; then
                while IFS=: read -r l_user l_group; do
                    [ "$l_user" = "UNKNOWN" ] && a_nouser+=("$l_file")
                    [ "$l_group" = "UNKNOWN" ] && a_nogroup+=("$l_file")
                    done <<(stat -Lc '%U:%G' "$l_file")
                fi
                done <<(find "$l_mount" -xdev \( "${a_path[@]}" \) \( -type f -o -type
d \) \( -nouser -o -nogroup \) -print0 2> /dev/null)
                done <<(findmnt -Dkerno fstype,target | awk '($1 !~
/^\\s*(nfs|proc|smb|vfat|iso9660|efivarfs|selinuxfs)/ && $2 !~
/^\\/run\\/user\\/){print $2}')
                if ! (( ${#a_nouser[@]} > 0 )); then
                    l_output="$l_output\n - No files or directories without a owner exist
on the local filesystem."
                else
                    l_output2="$l_output2\n - There are \"$(printf '%s'
"${#a_nouser[@]}")\" unowned files or directories on the system.\n - The
following is a list of unowned files and/or directories:\n$(printf '%s\n'
"${a_nouser[@]}")\n - end of list"
                fi
                if ! (( ${#a_nogroup[@]} > 0 )); then
                    l_output="$l_output\n - No files or directories without a group exist
on the local filesystem."
                else
                    l_output2="$l_output2\n - There are \"$(printf '%s'
"${#a_nogroup[@]}")\" ungrouped files or directories on the system.\n - The
following is a list of ungrouped files and/or directories:\n$(printf '%s\n'
"${a_nogroup[@]}")\n - end of list"
                fi
                unset a_path; unset a_arr ; unset a_nouser; unset a_nogroup # Remove
arrays
                if [ -z "$l_output2" ]; then # If l_output2 is empty, we pass
                    echo -e "\n- Audit Result:\n ** PASS **\n - * Correctly configured *
:\n$l_output\n"
                else
                    echo -e "\n- Audit Result:\n ** FAIL **\n - * Reasons for audit
failure * :\n$l_output2"
                    [ -n "$l_output" ] && echo -e "\n- * Correctly configured *
:\n$l_output\n"
                fi
            fi
        }
    }
}
```

**Note:** On systems with a large number of files and/or directories, this audit may be a long running process

## Remediation:

Remove or set ownership and group ownership of these files and/or directories to an active user on the system as appropriate.

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230326  
Rule ID: SV-230326r627750  
STIG ID: RHEL-08-010780  
Severity: CAT II

Vul ID: V-230327  
Rule ID: SV-230327r627750  
STIG ID: RHEL-08-010790  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1222, T1222.002            | TA0007  | M1022       |

### *7.1.13 Ensure SUID and SGID files are reviewed (Manual)*

**Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

**Description:**

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SUID or SGID program is to enable users to perform functions (such as changing their password) that require root privileges.

**Rationale:**

There are valid reasons for SUID and SGID programs, but it is important to identify and review such programs to ensure they are legitimate. Review the files returned by the action in the audit section and check to see if system binaries have a different checksum than what from the package. This is an indication that the binary may have been replaced.

## Audit:

Run the following script to generate a list of SUID and SGID files:

```
#!/usr/bin/env bash

{
    l_output="" l_output2=""
    a_suid=(); a_sgid=() # initialize arrays
    while IFS= read -r l_mount; do
        while IFS= read -r -d $'\0' l_file; do
            if [ -e "$l_file" ]; then
                l_mode="$(stat -Lc '%#a' "$l_file")"
                [ $(( $l_mode & 04000 )) -gt 0 ] && a_suid+=("$l_file")
                [ $(( $l_mode & 02000 )) -gt 0 ] && a_sgid+=("$l_file")
            fi
        done <<(find "$l_mount" -xdev -type f \( -perm -2000 -o -perm -4000 \)
-print0 2>/dev/null)
        done <<(findmnt -Dkerno fstype,target,options | awk '($1 !~
/^\/s*(nfs|proc|smb|vfat|iso9660|efivarfs|selinuxfs)/ && $2 !~
/^\/run\/user\/ // && $3 !~/noexec/ && $3 !~/nosuid/) {print $2}')
        if ! (( ${#a_suid[@]} > 0 )); then
            l_output="$l_output\n - No executable SUID files exist on the system"
        else
            l_output2="$l_output2\n - List of \"$(printf '%s' "${#a_suid[@]}")\"
SUID executable files:\n$(printf '%s\n' "${a_suid[@]}")\n - end of list -\n"
        fi
        if ! (( ${#a_sgid[@]} > 0 )); then
            l_output="$l_output\n - No SGID files exist on the system"
        else
            l_output2="$l_output2\n - List of \"$(printf '%s' "${#a_sgid[@]}")\"
SGID executable files:\n$(printf '%s\n' "${a_sgid[@]}")\n - end of list -\n"
        fi
        [ -n "$l_output2" ] && l_output2="$l_output2\n- Review the preceding
list(s) of SUID and/or SGID files to\n- ensure that no rogue programs have
been introduced onto the system.\n"
        unset a_arr; unset a_suid; unset a_sgid # Remove arrays
        # If l_output2 is empty, Nothing to report
        if [ -z "$l_output2" ]; then
            echo -e "\n- Audit Result:\n$l_output\n"
        else
            echo -e "\n- Audit Result:\n$l_output2\n"
            [ -n "$l_output" ] && echo -e "$l_output\n"
        fi
    fi
}
```

**Note:** on systems with a large number of files, this may be a long running process

## Remediation:

Ensure that no rogue SUID or SGID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the integrity of these binaries.

## References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5, AC-3, MP-2

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1548, T1548.001            | TA0004  | M1028       |

## 7.1.14 Ensure there are no ".shosts" files on the operating system (Automated)

### Profile Applicability:

- STIG

### Description:

There must be no .shosts files on the operating system.

### Rationale:

The ".shosts" files are used to configure host-based authentication for individual users or the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

### Audit:

Verify there are no ".shosts" files on the operating system with the following command:

```
# find / -name '*.shosts'
```

If any ".shosts" files are found, this is a finding.

### Remediation:

Remove any found ".shosts" files from the system.

```
# rm /[path]/[to]/[file]/.shosts
```

### References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230284  
Rule ID: SV-230284r627750  
STIG ID: RHEL-08-010470  
Severity: CAT I

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

### 7.1.15 Ensure there are no "shosts.equiv" files on the operating system (Automated)

#### Profile Applicability:

- STIG

#### Description:

There must be no shosts.equiv files on the operating system.

#### Rationale:

The "shosts.equiv" files are used to configure host-based authentication for the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

#### Audit:

Verify there are no "shosts.equiv" files on the operating with the following command:

```
# find / -name shosts.equiv
```

If a "shosts.equiv" file is found, this is a finding.

#### Remediation:

Remove any found "shosts.equiv" files from the system.

```
# rm /etc/ssh/shosts.equiv
```

#### References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230283  
Rule ID: SV-230283r627750  
STIG ID: RHEL-08-010460  
Severity: CAT I

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

## 7.1.16 Ensure system-wide shared library directories have mode 755 or less permissive (Automated)

### Profile Applicability:

- STIG

### Description:

System-wide shared library directories must have mode 755 or less permissive.

### Rationale:

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to RHEL 8 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals will be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

### Audit:

Run the following command to verify the system-wide shared library directories have mode "755" or less permissive with the following command:

```
# find /lib /lib64 /usr/lib /usr/lib64 -perm /022 -type d -exec stat -c "%n %a" '{}' \;
```

Nothing should be returned.

### Remediation:

Configure the library directories to be protected from unauthorized access. Run the following command, replacing "[DIRECTORY]" with any library directory with a mode more permissive than 755.

```
# chmod 755 [DIRECTORY]
```

### References:

1. NIST SP 800-53 :: CM-5 (6)
2. NIST SP 800-53A :: CM-5 (6).1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-251707  
Rule ID: SV-251707r809345  
STIG ID: RHEL-08-010331  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## *7.1.17 Ensure system-wide shared library directories must be owned by root (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

Library directories must be owned by root.

### **Rationale:**

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to RHEL 8 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals will be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

### **Audit:**

Run the following command to verify the system-wide shared library directories are owned by "root" with the following command:

```
# find /lib /lib64 /usr/lib /usr/lib64 ! -user root -type d -exec stat -c "%n %U" '{}' \;
```

Nothing should be returned

### **Remediation:**

Configure the system-wide shared library directories within (/lib, /lib64, /usr/lib and /usr/lib64) to be protected from unauthorized access.

Run the following command, replacing "[DIRECTORY]" with any library directory not owned by **root**:

```
# chown root [DIRECTORY]
```

### **References:**

1. NIST SP 800-53 :: CM-5 (6)
2. NIST SP 800-53A :: CM-5 (6).1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-251708  
Rule ID: SV-251708r810012  
STIG ID: RHEL-08-010341  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## *7.1.18 Ensure the system-wide shared library directories are group-owned by root or a system account (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

System-wide shared library directories must be group-owned by root or a system account.

### **Rationale:**

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to RHEL 8 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals will be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

### **Audit:**

Run the following command to verify the system-wide shared library directories are group-owned by root:

```
# find /lib /lib64 /usr/lib /usr/lib64 ! -group root -type d -exec stat -c "%n %G" '{}' \;
```

Nothing should be returned.

### **Remediation:**

Configure the system-wide shared library directories (/lib, /lib64, /usr/lib and /usr/lib64) to be protected from unauthorized access.

Run the following command, replacing "[DIRECTORY]" with any library directory not group-owned by root:

```
# chgrp root [DIRECTORY]
```

### **References:**

1. NIST SP 800-53 :: CM-5 (6)
2. NIST SP 800-53A :: CM-5 (6).1



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-251709  
Rule ID: SV-251709r810014  
STIG ID: RHEL-08-010351  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## 7.1.19 Ensure world-writable directories owner is configured (Manual)

### Profile Applicability:

- STIG

### Description:

All world-writable directories must be owned by root, sys, bin, or an application user.

### Rationale:

If a world-writable directory is not owned by root, sys, bin, or an application User Identifier (UID), unauthorized users may be able to modify files created by others.

The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage, (e.g., /tmp), and for directories requiring global read/write access.

### Audit:

The following command will discover and print world-writable directories that are not owned by a system account, given the assumption that only system accounts have a UID lower than 1000. Run it once for each local partition [PART]:

```
# find [PART] -xdev -type d -perm -0002 -uid +999 -print
```

If there is output, this is a finding.

### Remediation:

All directories in local partitions which are world-writable should be owned by root or another system account. If any world-writable directories are not owned by a system account, this should be investigated. Following this, the files should be deleted or assigned to an appropriate group.

### References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230318  
Rule ID: SV-230318r743960  
STIG ID: RHEL-08-010700  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## 7.1.20 Ensure world-writable directories group-owner is configured (Manual)

### Profile Applicability:

- STIG

### Description:

All world-writable directories must be group-owned by root, sys, bin, or an application group.

### Rationale:

If a world-writable directory is not group-owned by root, sys, bin, or an application Group Identifier (GID), unauthorized users may be able to modify files created by others.

The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage, (e.g., /tmp), and for directories requiring global read/write access.

### Audit:

The following command will discover and print world-writable directories that are not group-owned by a system account, given the assumption that only system accounts have a GID lower than 1000. Run it once for each local partition [PART]:

```
# find [PART] -xdev -type d -perm -0002 -gid +999 -print
```

If there is output, this is a finding.

### Remediation:

All directories in local partitions which are world-writable must be group-owned by root or another system account. If any world-writable directories are not group-owned by a system account, this must be investigated. Following this, the directories must be deleted or assigned to an appropriate group.

### References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230319  
Rule ID: SV-230319r743961  
STIG ID: RHEL-08-010710  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## 7.1.21 Ensure local initialization files do not execute world-writable programs (Manual)

### Profile Applicability:

- STIG

### Description:

Local operating system initialization files must not execute world-writable programs.

### Rationale:

If user start-up files execute world-writable programs, especially in unprotected directories, they could be maliciously modified to destroy user files or otherwise compromise the system at the user level. If the system is compromised at the user level, it is easier to elevate privileges to eventually compromise the system at the root and network level.

### Audit:

Verify that local initialization files do not execute world-writable programs.

Check the system for world-writable files.

The following command will discover and print world-writable files. Run it once for each local partition [PART]:

```
# find [PART] -xdev -type f -perm -0002 -print
```

For all files listed, check for their presence in the local initialization files with the following commands:

Note: The example will be for a system that is configured to create user home directories in the "/home" directory.

```
# grep <file> /home/*/*.*
```

If any local initialization files are found to reference world-writable files, this is a finding.

### Remediation:

Set the mode on files being executed by the local initialization files with the following command:

```
# chmod 0755 <file>
```

### References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230309  
Rule ID: SV-230309r627750  
STIG ID: RHEL-08-010660  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### *7.1.22 Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are mode 0755 or more restrictive (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

System commands must have mode "0755" or less permissive.

#### **Rationale:**

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals will be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

#### **Audit:**

Verify the system commands contained in the following directories have mode "0755" or less permissive with the following command:

```
# find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin -perm /0022 -exec ls -l {} \;
```

If any system commands are found to be group-writable or world-writable, this is a finding.

#### **Remediation:**

Configure the system commands to be protected from unauthorized access. Run the following command, replacing "[FILE]" with any system command with a mode more permissive than "0755".

```
# chmod 0755 [FILE]
```

#### **References:**

1. NIST SP 800-53 :: CM-5 (6)
2. NIST SP 800-53A :: CM-5 (6).1



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230257  
Rule ID: SV-230257r792862  
STIG ID: RHEL-08-010300  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

### *7.1.23 Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are owned by root (Automated)*

**Profile Applicability:**

- STIG

**Description:**

System commands must be owned by root.

**Rationale:**

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals will be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

**Audit:**

Verify the system commands contained in the following directories are owned by "root" with the following command:

```
# find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -  
user root -exec ls -l {} \;
```

If any system commands are returned, this is a finding.

## Remediation:

Configure the system commands to be protected from unauthorized access.  
Run the following command, replacing "[FILE]" with any system command file not owned by "root".

```
# chown root [FILE]
```

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230258  
Rule ID: SV-230258r627750  
STIG ID: RHEL-08-010310  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |   |   |   |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## *7.1.24 Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are group-owned by root (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

System commands must be group-owned by root or a system account.

### **Rationale:**

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals will be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

### **Audit:**

Verify the system commands contained in the following directories are group-owned by "root" with the following command:

```
# find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -  
group root -exec ls -l {} \;
```

If any system commands are returned and is not owned by a required system account, this is a finding.

### **Remediation:**

Configure the system commands to be protected from unauthorized access. Run the following command, replacing "[FILE]" with any system command file not group-owned by "root" or a required system account.

```
# chgrp root [FILE]
```

### **References:**

1. NIST SP 800-53 :: CM-5 (6)
2. NIST SP 800-53A :: CM-5 (6).1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230259  
Rule ID: SV-230259r792864  
STIG ID: RHEL-08-010320  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## *7.1.25 Ensure the system-wide shared library files are mode 0755 or more restrictive (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

Library files must have mode "0755" or less permissive.

### **Rationale:**

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals will be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

### **Audit:**

Verify the system-wide shared library files contained in the following directories have mode "0755" or less permissive with the following command:

```
# find -L /lib /lib64 /usr/lib /usr/lib64 -perm /0022 -type f -exec ls -l {} \;
```

If any system-wide shared library file is found to be group-writable or world-writable, this is a finding.

### **Remediation:**

Configure the library files to be protected from unauthorized access. Run the following command, replacing "[FILE]" with any library file with a mode more permissive than 0755.

```
# chmod 0755 [FILE]
```

### **References:**

1. NIST SP 800-53 :: CM-5 (6)
2. NIST SP 800-53A :: CM-5 (6).1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230260  
Rule ID: SV-230260r792867  
STIG ID: RHEL-08-010330  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## 7.1.26 Ensure the system-wide shared library files are owned by root (Automated)

### Profile Applicability:

- STIG

### Description:

Library files must be owned by root.

### Rationale:

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals will be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

### Audit:

Verify the system-wide shared library files are owned by "root" with the following command:

```
# find -L /lib /lib64 /usr/lib /usr/lib64 ! -user root -exec ls -l {} \;
```

If any system wide shared library file is returned, this is a finding.

### Remediation:

Configure the system-wide shared library files (/lib, /lib64, /usr/lib and /usr/lib64) to be protected from unauthorized access.

Run the following command, replacing "[FILE]" with any library file not owned by "root".

```
# chown root [FILE]
```

### References:

1. NIST SP 800-53 :: CM-5 (6)
2. NIST SP 800-53A :: CM-5 (6).1



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230261  
Rule ID: SV-230261r627750  
STIG ID: RHEL-08-010340  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## *7.1.27 Ensure the system-wide shared library files are group-owned by root (Automated)*

### **Profile Applicability:**

- STIG

### **Description:**

Library files must be group-owned by root or a system account.

### **Rationale:**

If the operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges. Only qualified and authorized individuals will be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

### **Audit:**

Verify the system-wide shared library files are group-owned by "root" with the following command:

```
# find -L /lib /lib64 /usr/lib /usr/lib64 ! -group root -exec ls -l {} \;
```

If any system wide shared library file is returned and is not group-owned by a required system account, this is a finding.

### **Remediation:**

Configure the system-wide shared library files (/lib, /lib64, /usr/lib and /usr/lib64) to be protected from unauthorized access.

Run the following command, replacing "[FILE]" with any library file not group-owned by "root".

```
# chgrp root [FILE]
```

### **References:**

1. NIST SP 800-53 :: CM-5 (6)
2. NIST SP 800-53A :: CM-5 (6).1

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230262  
Rule ID: SV-230262r627750  
STIG ID: RHEL-08-010350  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## 7.2 Local User and Group Settings

This section provides guidance on securing aspects of the local users and groups.

**Note:** The recommendations in this section check local users and groups. Any users or groups from other sources such as LDAP will not be audited. In a domain environment similar checks should be performed against domain users and groups.

## 7.2.1 Ensure accounts in /etc/passwd use shadowed passwords (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Local accounts can use shadowed passwords. With shadowed passwords, the passwords are saved in the shadow password file, `/etc/shadow`, encrypted by a salted one-way hash. Accounts with a shadowed password have an `x` in the second field in `/etc/passwd`.

### Rationale:

The `/etc/passwd` file also contains information like user ID's and group ID's that are used by many system programs. Therefore, the `/etc/passwd` file must remain world readable. In spite of encoding the password with a randomly-generated one-way hash function, an attacker could still break the system if they got access to the `/etc/passwd` file. This can be mitigated by using shadowed passwords, thus moving the passwords in the `/etc/passwd` file to `/etc/shadow`. The `/etc/shadow` file is set so only root will be able to read and write. This helps mitigate the risk of an attacker gaining access to the encoded passwords with which to perform a dictionary attack.

### Note:

- All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.
- A user account with an empty second field in `/etc/passwd` allows the account to be logged into by providing only the username.

### Audit:

Run the following command and verify that no output is returned:

```
# awk -F: '($2 != "x" ) { print "User: \"" $1 "\" is not set to shadowed passwords "}' /etc/passwd
```

### Remediation:

Run the following command to set accounts to use shadowed passwords and migrate passwords in `/etc/passwd` to `/etc/shadow`:

```
# pwconv
```

Investigate to determine if the account is logged in and what it is being used for, to determine if it needs to be forced off.

## References:

1. NIST SP 800-53 Rev. 5: IA-5
2. PWCONV(8)

## Additional Information:

The **pwconv** command creates shadow from **passwd** and an optionally existing **shadow**.

- The **pwunconv** command creates **passwd** from **passwd** and **shadow** and then removes **shadow**.
- The **grpconv** command creates **gshadow** from **group** and an optionally existing **gshadow**.
- The **grpunconv** command creates **group** from **group** and **gshadow** and then removes **gshadow**.

These four programs all operate on the normal and shadow password and group files: **/etc/passwd**, **/etc/group**, **/etc/shadow**, and **/etc/gshadow**.

Each program acquires the necessary locks before conversion. **pwconv** and **grpconv** are similar. First, entries in the shadowed file which don't exist in the main file are removed. Then, shadowed entries which don't have **x'** as the password in the main file are updated. Any missing shadowed entries are added. Finally, passwords in the main file are replaced with **x'**. These programs can be used for initial conversion as well to update the shadowed file if the main file is edited by hand.

**pwconv** will use the values of **PASS\_MIN\_DAYS**, **PASS\_MAX\_DAYS**, and **PASS\_WARN\_AGE** from **/etc/login.defs** when adding new entries to **/etc/shadow**.

**pwunconv** and **grpunconv** are similar. Passwords in the main file are updated from the shadowed file. Entries which exist in the main file but not in the shadowed file are left alone. Finally, the shadowed file is removed. Some password aging information is lost by **pwunconv**. It will convert what it can.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.11 <u>Encrypt Sensitive Data at Rest</u></b><br>Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data. |      |  |  |

| Controls Version | Control                                                                                                                               | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v7               | 16.4 <u>Encrypt or Hash all Authentication Credentials</u><br>Encrypt or hash with a salt all authentication credentials when stored. |      |  |  |

#### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1003, T1003.008            | TA0003  | M1027       |

## 7.2.2 Ensure /etc/shadow password fields are not empty (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

### Description:

An account with an empty password field means that anybody may log in as that user without providing a password.

### Rationale:

All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.

### Audit:

Run the following command and verify that no output is returned:

```
# awk -F: '($2 == "" ) { print $1 " does not have a password "}' /etc/shadow
```

### Remediation:

If any accounts in the `/etc/shadow` file do not have a password, run the following command to lock the account until it can be determined why it does not have a password:

```
# passwd -l <username>
```

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be forced off.

### References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)



## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-251706  
Rule ID: SV-251706r809342  
STIG ID: RHEL-08-010121  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>5.2 Use Unique Passwords</b><br>Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA. |  |  |  |
| v7               | <b>4.4 Use Unique Passwords</b><br>Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.                                    |                                                                                     |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1078, T1078.001, T1078.003 | TA0003  | M1027       |

### 7.2.3 Ensure all groups in /etc/passwd exist in /etc/group (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

Over time, system administration errors and changes can lead to groups being defined in **/etc/passwd** but not in **/etc/group**.

#### Rationale:

Groups defined in the **/etc/passwd** file but not in the **/etc/group** file pose a threat to system security since group permissions are not properly managed.

#### Audit:

Run the following script to verify all GIDs in **/etc/passwd** exist in **/etc/group**:

```
#!/usr/bin/env bash

{
  a_passwd_group_gid=("${awk -F: '{print $4}' /etc/passwd | sort -u}")
  a_group_gid=("${awk -F: '{print $3}' /etc/group | sort -u}")
  a_passwd_group_diff=("${printf '%s\n' "${a_group_gid[@]}"
"${a_passwd_group_gid[@]}" | sort | uniq -u}")
  while IFS= read -r l_gid; do
    awk -F: '($4 == '"$l_gid"') {print "  - User: \"" $1 "\" has GID: \""
$4 "\" which does not exist in /etc/group" }' /etc/passwd
  done <<("${printf '%s\n' "${a_passwd_group_gid[@]}"
"${a_passwd_group_diff[@]}" | sort | uniq -D | uniq)
  unset a_passwd_group_gid; unset a_group_gid; unset a_passwd_group_diff
}
```

Nothing should be returned

#### Remediation:

Analyze the output of the Audit step above and perform the appropriate action to correct any discrepancies found.

#### References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                        | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications. |  |  |  |
| v8               | <b>14.6 <u>Train Workforce Members on Recognizing and Reporting Security Incidents</u></b><br>Train workforce members to be able to recognize a potential incident and be able to report such an incident.                                                     |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1222, T1222.002            | TA0003  | M1027       |

## 7.2.4 Ensure shadow group is empty (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The shadow group allows system programs which require access the ability to read the `/etc/shadow` file. No users should be assigned to the shadow group.

### Rationale:

Any users assigned to the shadow group would be granted read access to the `/etc/shadow` file. If attackers can gain read access to the `/etc/shadow` file, they can easily run a password cracking program against the hashed passwords to break them. Other security information that is stored in the `/etc/shadow` file (such as expiration) could also be useful to subvert additional user accounts.

### Audit:

Run the following commands and verify no results are returned:

```
# awk -F: '($1=="shadow") {print $NF}' /etc/group
# awk -F: '($4 == '"$(getent group shadow | awk -F: '{print $3}' | xargs)'"')
{print "  - user: \"" $1 "\" primary group is the shadow group"}' /etc/passwd
```

### Remediation:

Run the following command to remove all users from the shadow group

```
# sed -ri 's/^(^shadow:[^:]*:[^:]*:)([^\:]+$)/\1/' /etc/group
```

Change the primary group of any users with shadow as their primary group.

```
# usermod -g <primary group> <user>
```

### References:

1. NIST SP 800-53 Rev. 5: IA-5

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1003, T1003.008            | TA0005  | M1022       |

## 7.2.5 Ensure no duplicate UIDs exist (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation
- STIG

### Description:

Although the **useradd** program will not let you create a duplicate User ID (UID), it is possible for an administrator to manually edit the **/etc/passwd** file and change the UID field.

### Rationale:

Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.

Satisfies: SRG-OS-000104-GPOS-00051, SRG-OS-000121-GPOS-00062, SRG-OS-000042-GPOS-00020

### Audit:

Run the following script and verify no results are returned:

```
#!/usr/bin/env bash

{
  while read -r l_count l_uid; do
    if [ "$l_count" -gt 1 ]; then
      echo -e "Duplicate UID: \"$l_uid\" Users: \"$(awk -F: '($3 == $l_uid) { print $1 }' n=$l_uid /etc/passwd | xargs)\""
    fi
    done <<(cut -f3 -d":" /etc/passwd | sort -n | uniq -c)
  }
}
```

### Remediation:

Based on the results of the audit script, establish unique UIDs and review all files owned by the shared UIDs to determine which UID they are supposed to belong to.

### References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5
2. NIST SP 800-53A :: IA-2.1

### Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: V-230371  
Rule ID: SV-230371r627750  
STIG ID: RHEL-08-020240  
Severity: CAT II

### MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1078, T1078.001, T1078.003 | TA0005  | M1027       |

## 7.2.6 Ensure no duplicate GIDs exist (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Although the **groupadd** program will not let you create a duplicate Group ID (GID), it is possible for an administrator to manually edit the **/etc/group** file and change the GID field.

### Rationale:

User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.

### Audit:

Run the following script and verify no results are returned:

```
#!/usr/bin/env bash

{
    while read -r l_count l_gid; do
        if [ "$l_count" -gt 1 ]; then
            echo -e "Duplicate GID: \"$l_gid\" Groups: \"$(awk -F: '($3 == n) {
print $1 }' n=$l_gid /etc/group | xargs)\""
            fi
            done <<(cut -f3 -d":" /etc/group | sort -n | uniq -c)
        }
    }
```

### Remediation:

Based on the results of the audit script, establish unique GIDs and review all files owned by the shared GID to determine which group they are supposed to belong to.

### References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

### Additional Information:

You can also use the **grpck** command to check for other inconsistencies in the **/etc/group** file.



**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1078, T1078.001, T1078.003 | TA0005  | M1027       |

## 7.2.7 Ensure no duplicate user names exist (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Although the **useradd** program will not let you create a duplicate user name, it is possible for an administrator to manually edit the **/etc/passwd** file and change the user name.

### Rationale:

If a user is assigned a duplicate user name, it will create and have access to files with the first UID for that username in **/etc/passwd**. For example, if "test4" has a UID of 1000 and a subsequent "test4" entry has a UID of 2000, logging in as "test4" will use UID 1000. Effectively, the UID is shared, which is a security problem.

### Audit:

Run the following script and verify no results are returned:

```
#!/usr/bin/env bash

{
  while read -r l_count l_user; do
    if [ "$l_count" -gt 1 ]; then
      echo -e "Duplicate User: \"$l_user\" Users: \"$(awk -F: '($1 == n) {
print $1 }' n=$l_user /etc/passwd | xargs)\""
    fi
  done <<(cut -f1 -d":" /etc/group | sort -n | uniq -c)
}
```

### Remediation:

Based on the results of the audit script, establish unique user names for the users. File ownerships will automatically reflect the change as long as the users have unique UIDs.

### References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

**MITRE ATT&CK Mappings:**

| <b>Techniques / Sub-techniques</b> | <b>Tactics</b> | <b>Mitigations</b> |
|------------------------------------|----------------|--------------------|
| T1078, T1078.001,<br>T1078.003     | TA0004         | M1027              |

## 7.2.8 Ensure no duplicate group names exist (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Although the **groupadd** program will not let you create a duplicate group name, it is possible for an administrator to manually edit the **/etc/group** file and change the group name.

### Rationale:

If a group is assigned a duplicate group name, it will create and have access to files with the first GID for that group in **/etc/group**. Effectively, the GID is shared, which is a security problem.

### Audit:

Run the following script and verify no results are returned:

```
#!/usr/bin/env bash

{
  while read -r l_count l_group; do
    if [ "$l_count" -gt 1 ]; then
      echo -e "Duplicate Group: \"$l_group\" Groups: \"$(awk -F: '($1 == n) { print $1 }' n=$l_group /etc/group | xargs)\""
      fi
    done <<(cut -f1 -d":" /etc/group | sort -n | uniq -c)
  }
```

### Remediation:

Based on the results of the audit script, establish unique names for the user groups. File group ownerships will automatically reflect the change as long as the groups have unique GIDs.

### References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1078, T1078.001, T1078.003 | TA0004  | M1027       |

## *7.2.9 Ensure local interactive user home directories are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation
- STIG

### **Description:**

The user home directory is space defined for the particular user to set local environment variables and to store personal files. While the system administrator can establish secure permissions for users' home directories, the users can easily override these. Users can be defined in `/etc/passwd` without a home directory or with a home directory that does not actually exist.

### **Rationale:**

Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory. Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges. If the user's home directory does not exist or is unassigned, the user will be placed in "/" and will not be able to write any files or have local environment variables set.

### **Audit:**

Run the following script to Ensure:

- local interactive user home directories exist
- Ensure local interactive users own their home directories
- Ensure local interactive user home directories are mode 750 or more restrictive

```
#!/usr/bin/env bash

{
    l_output="" l_output2="" l_heout2="" l_hoout2="" l_haout2=""
    l_valid_shells="^($( awk -F\ / '$NF != "nologin" {print}' /etc/shells | sed
-rn '/^\//{s,/,\ \ \ \/,g;p}' | paste -s -d '|' - ))$"
    unset a_uarr && a_uarr=() # Clear and initialize array
    while read -r l_epu l_eph; do # Populate array with users and user home
location
        a_uarr+=("$l_epu $l_eph")
        done <<< "$ (awk -v pat="$l_valid_shells" -F: '$(NF) ~ pat { print $1 " "
$(NF-1) }' /etc/passwd)"
        l_asize="${#a_uarr[@]}" # Here if we want to look at number of users
before proceeding
        [ "$l_asize" -gt "10000" ] && echo -e "\n ** INFO **\n - \"$l_asize\"
Local interactive users found on the system\n - This may be a long running
check\n"
        while read -r l_user l_home; do
            if [ -d "$l_home" ]; then
                l_mask='0027'
                l_max="$( printf '%o' $(( 0777 & ~$l_mask )) )"
                while read -r l_own l_mode; do
                    [ "$l_user" != "$l_own" ] && l_hoout2="$l_hoout2\n - User:
\"$l_user\" Home \"$l_home\" is owned by: \"$l_own\""
                    if [ $(( $l_mode & $l_mask )) -gt 0 ]; then
                        l_haout2="$l_haout2\n - User: \"$l_user\" Home \"$l_home\" is
mode: \"$l_mode\" should be mode: \"$l_max\" or more restrictive"
                    fi
                    done <<< "$(stat -Lc '%U %#a' "$l_home")"
                else
                    l_heout2="$l_heout2\n - User: \"$l_user\" Home \"$l_home\" Doesn't
exist"
                fi
                done <<< "$(printf '%s\n' "${a_uarr[@]}")"
                [ -z "$l_heout2" ] && l_output="$l_output\n - home directories exist" ||
l_output2="$l_output2$l_heout2"
                [ -z "$l_hoout2" ] && l_output="$l_output\n - own their home directory"
|| l_output2="$l_output2$l_hoout2"
                [ -z "$l_haout2" ] && l_output="$l_output\n - home directories are mode:
\"$l_max\" or more restrictive" || l_output2="$l_output2$l_haout2"
                [ -n "$l_output" ] && l_output=" - All local interactive users:$l_output"
                if [ -z "$l_output2" ]; then # If l_output2 is empty, we pass
                    echo -e "\n- Audit Result:\n ** PASS **\n - * Correctly configured *
:\n$l_output"
                else
                    echo -e "\n- Audit Result:\n ** FAIL **\n - * Reasons for audit
failure * :\n$l_output2"
                    [ -n "$l_output" ] && echo -e "\n- * Correctly configured *
:\n$l_output"
                fi
            fi
        }
}
```

## Remediation:

If a local interactive users' home directory is undefined and/or doesn't exist, follow local site policy and perform one of the following:

- Lock the user account
- Remove the user from the system
- create a directory for the user. If undefined, edit `/etc/passwd` and add the absolute path to the directory to the last field of the user.

Run the following script to:

- Remove excessive permissions from local interactive users home directories
- Update the home directory's owner



```

#!/usr/bin/env bash

{
    l_output2=""
    l_valid_shells="^( $( awk -F\ / ' $NF != "nologin" {print}' /etc/shells | sed
-rn '/^\//{s,/,\//,g;p}' | paste -s -d '|' - ) ) $"
    unset a_uarr && a_uarr=() # Clear and initialize array
    while read -r l_epu l_eph; do # Populate array with users and user home
location
        a_uarr+=("$l_epu $l_eph")
        done <<< "$(awk -v pat="$l_valid_shells" -F: '$(NF) ~ pat { print $1 " "
$(NF-1) }' /etc/passwd)"
        l_asize="${#a_uarr[@]}" # Here if we want to look at number of users
before proceeding
        [ "$l_asize" -gt "10000" ] && echo -e "\n ** INFO **\n - \"$l_asize\"
Local interactive users found on the system\n - This may be a long running
process\n"
        while read -r l_user l_home; do
            if [ -d "$l_home" ]; then
                l_mask='0027'
                l_max="$( printf '%o' $( ( 0777 & ~$l_mask ) )"
                while read -r l_own l_mode; do
                    if [ "$l_user" != "$l_own" ]; then
                        l_output2="$l_output2\n - User: \"$l_user\" Home \"$l_home\"
is owned by: \"$l_own\" \n - changing ownership to: \"$l_user\" \n"
                        chown "$l_user" "$l_home"
                    fi
                    if [ $( ( $l_mode & $l_mask ) ) -gt 0 ]; then
                        l_output2="$l_output2\n - User: \"$l_user\" Home \"$l_home\"
is mode: \"$l_mode\" should be mode: \"$l_max\" or more restrictive\n -
removing excess permissions\n"
                        chmod g-w,o-rwx "$l_home"
                    fi
                done <<< "$(stat -Lc '%U %#a' "$l_home")"
            else
                l_output2="$l_output2\n - User: \"$l_user\" Home \"$l_home\"
Doesn't exist\n - Please create a home in accordance with local site
policy"
            fi
            done <<< "$(printf '%s\n' "${a_uarr[@]}")"
            if [ -z "$l_output2" ]; then # If l_output2 is empty, we pass
                echo -e " - No modification needed to local interactive users home
directories"
            else
                echo -e "\n$l_output2"
            fi
        }
}

```

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 14 Benchmark Date: 24 APR 2024

Vul ID: 230320  
Rule ID: SV-230320r627750  
STIG ID: RHEL-08-010720  
Severity: CAT II

GROUP ID: V-230321  
RULE ID: SV-230321r627750  
STIG ID: RHEL-08-010730  
SEVERITY: CAT II

Vul ID: V-230323  
Rule ID: SV-230323r627750  
STIG ID: RHEL-08-010750  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 Protect Information through Access Control Lists</b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## MITRE ATT&CK Mappings:

| Techniques / Sub-techniques | Tactics | Mitigations |
|-----------------------------|---------|-------------|
| T1222, T1222.002            | TA0005  | M1022       |

## 7.2.10 Ensure local interactive user dot files access is configured (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

While the system administrator can establish secure permissions for users' "dot" files, the users can easily override these.

- **.forward** file specifies an email address to forward the user's mail to.
- **.rhost** file provides the "remote authentication" database for the rcp, rlogin, and rsh commands and the rcmd() function. These files bypass the standard password-based user authentication mechanism. They specify remote hosts and users that are considered trusted (i.e. are allowed to access the local system without supplying a password)
- **.netrc** file contains data for logging into a remote host or passing authentication to an API.
- **.bash\_history** file keeps track of the user's commands.

### Rationale:

User configuration files with excessive or incorrect access may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

### Audit:

Run the following script to verify local interactive user dot files:

- Don't include **.forward**, **.rhost**, or **.netrc** files
- Are mode 0644 or more restrictive
- Are owned by the local interactive user
- Are group owned by the user's primary group
- **.bash\_history** is mode 0600 or more restrictive

**Note:** If a **.netrc** file is required, and follows local site policy, it should be mode **0600** or more restrictive.

```

#!/usr/bin/env bash

{
    a_output2=(); a_output3=()
    l_maxsize="1000" # Maximum number of local interactive users before
warning (Default 1,000)
    l_valid_shells="^($( awk -F\ / ' $NF != "nologin" {print}' /etc/shells | sed
-rn '/^\/\/{s,/,\ \ \ \/,g;p}' | paste -s -d '|' - ))$"
    a_user_and_home=() # Create array with local users and their home
directories
    while read -r l_local_user l_local_user_home; do # Populate array with
users and user home location
        [[ -n "$l_local_user" && -n "$l_local_user_home" ]] &&
a_user_and_home+=("$l_local_user:$l_local_user_home")
        done <<< "$ (awk -v pat="$l_valid_shells" -F: '$(NF) ~ pat { print $1 " "
$(NF-1) }' /etc/passwd)"
        l_asize="${#a_user_and_home[@]}" # Here if we want to look at number of
users before proceeding
        [ "${#a_user_and_home[@]}" -gt "$l_maxsize" ] && printf '%s\n' "" " **
INFO **" \
        " - \"$l_asize\" Local interactive users found on the system" \
        " - This may be a long running check" ""
        file_access_chk()
        {
            a_access_out=()
            l_max="$( printf '%o' $(( 0777 & ~$l_mask)) )"
            if [ $(( $l_mode & $l_mask )) -gt 0 ]; then
                a_access_out+=(" - File: \"$l_hdfilename\" is mode: \"$l_mode\" and
should be mode: \"$l_max\" or more restrictive")
            fi
            if [[ ! "$l_owner" =~ ($l_user) ]]; then
                a_access_out+=(" - File: \"$l_hdfilename\" owned by: \"$l_owner\" and
should be owned by \"${l_user} // or \"")
            fi
            if [[ ! "$l_gowner" =~ ($l_group) ]]; then
                a_access_out+=(" - File: \"$l_hdfilename\" group owned by:
\"$l_gowner\" and should be group owned by \"${l_group} // or \"")
            fi
        }
        while IFS=: read -r l_user l_home; do
            a_dot_file=(); a_netrc=(); a_netrc_warn=(); a_bhout=(); a_hdirout=()
            if [ -d "$l_home" ]; then
                l_group="$(id -gn "$l_user" | xargs)"; l_group="${l_group} // ||"
                while IFS= read -r -d $'\0' l_hdfilename; do
                    while read -r l_mode l_owner l_gowner; do
                        case "$(basename "$l_hdfilename")" in
                            .forward | .rhost )
                                a_dot_file+=(" - File: \"$l_hdfilename\" exists") ;;
                            .netrc )
                                l_mask='0177'; file_access_chk
                                if [ "${#a_access_out[@]}" -gt 0 ]; then
                                    a_netrc+=("${a_access_out[@]}")
                                else
                                    a_netrc_warn+=(" - File: \"$l_hdfilename\" exists")
                                fi ;;
                            .bash_history )
                                l_mask='0177'; file_access_chk

```

```

[ "${#a_access_out[@]}" -gt 0 ] &&
a_bhout+=("${a_access_out[@]}") ;;
* )
    l_mask='0133'; file_access_chk
    [ "${#a_access_out[@]}" -gt 0 ] &&
a_hdirout+=("${a_access_out[@]}") ;;
esac
done <<(stat -Lc '%#a %U %G' "$l_hdfilename")
done <<(find "$l_home" -xdev -type f -name '.*' -print0)
fi
if [[ "${#a_dot_file[@]}" -gt 0 || "${#a_netrc[@]}" -gt 0 ||
"${#a_bhout[@]}" -gt 0 || "${#a_hdirout[@]}" -gt 0 ]]; then
    a_output2+=(" - User: \"$l_user\" Home Directory: \"$l_home\"")
    "${a_dot_file[@]}" "${a_netrc[@]}" "${a_bhout[@]}" "${a_hdirout[@]}"
fi
[ "${#a_netrc_warn[@]}" -gt 0 ] && a_output3+=(" - User: \"$l_user\"
Home Directory: \"$l_home\"") "${a_netrc_warn[@]}"
done <<< "$(printf '%s\n' "${a_user_and_home[@]}")"
if [ "${#a_output2[@]}" -le 0 ]; then # If l_output2 is empty, we pass
    [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' " ** WARNING **"
"${a_output3[@]}"
    printf '%s\n' "- Audit Result:" " ** PASS **"
else
    printf '%s\n' "- Audit Result:" " ** FAIL **" " - * Reasons for audit
failure * : "${a_output2[@]}" ""
    [ "${#a_output3[@]}" -gt 0 ] && printf '%s\n' " ** WARNING **"
"${a_output3[@]}"
fi
}

```

## Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user dot file permissions and determine the action to be taken in accordance with site policy.

The following script will:

- remove excessive permissions on **dot** files within interactive users' home directories
- change ownership of **dot** files within interactive users' home directories to the user
- change group ownership of **dot** files within interactive users' home directories to the user's primary group
- list **.forward** and **.rhost** files to be investigated and manually deleted

```

#!/usr/bin/env bash

{
    a_output2=(); a_output3=()
    l_maxsize="1000" # Maximum number of local interactive users before
warning (Default 1,000)
    l_valid_shells="^($( awk -F\| ' $NF != "nologin" {print}' /etc/shells | sed
-rn '/^\\/{s/,/,\\\\/,g;p}' | paste -s -d '|' - ))$"
    a_user_and_home=() # Create array with local users and their home
directories
    while read -r l_local_user l_local_user_home; do # Populate array with
users and user home location
        [[ -n "$l_local_user" && -n "$l_local_user_home" ]] &&
a_user_and_home+=("$l_local_user:$l_local_user_home")
        done <<< "$ (awk -v pat="$l_valid_shells" -F: '$(NF) ~ pat { print $1 " "
$(NF-1) }' /etc/passwd)"
        l_asize="${#a_user_and_home[@]}" # Here if we want to look at number of
users before proceeding
        [ "${#a_user_and_home[@]}" -gt "$l_maxsize" ] && printf '%s\n' "" " **
INFO **" \
        " - \"$l_asize\" Local interactive users found on the system" \
        " - This may be a long running check" ""
        file_access_fix()
        {
            a_access_out=()
            l_max="$( printf '%o' $(( 0777 & ~$l_mask)) )"
            if [ $(( $l_mode & $l_mask )) -gt 0 ]; then
                printf '%s\n' "" " - File: \"$l_hdfilename\" is mode: \"$l_mode\" and
should be mode: \"$l_max\" or more restrictive" \
                "      Updating file: \"$l_hdfilename\" to be mode: \"$l_max\" or more
restrictive"
                chmod "$l_change" "$l_hdfilename"
            fi
            if [[ ! "$l_owner" =~ ($l_user) ]]; then
                printf '%s\n' "" " - File: \"$l_hdfilename\" owned by: \"$l_owner\" and
should be owned by \"${l_user//|/ or }\"" \
                "      Updating file: \"$l_hdfilename\" to be owned by \"${l_user//|/ or
}\""
                chown "$l_user" "$l_hdfilename"
            fi
            if [[ ! "$l_gowner" =~ ($l_group) ]]; then
                printf '%s\n' "" " - File: \"$l_hdfilename\" group owned by:
\"$l_gowner\" and should be group owned by \"${l_group//|/ or }\"" \
                "      Updating file: \"$l_hdfilename\" to be group owned by
\"${l_group//|/ or }\""
                chgrp "$l_group" "$l_hdfilename"
            fi
        }
        while IFS=: read -r l_user l_home; do
            a_dot_file=(); a_netrc=(); a_netrc_warn=(); a_bhout=(); a_hdirout=()
            if [ -d "$l_home" ]; then
                l_group="$(id -gn "$l_user" | xargs)"; l_group="${l_group//|/}"
                while IFS= read -r -d $'\0' l_hdfilename; do
                    while read -r l_mode l_owner l_gowner; do
                        case "$(basename "$l_hdfilename")" in
                            .forward | .rhost )
                                a_dot_file+=(" - File: \"$l_hdfilename\" exists" "

```

```
Please review and manually delete this file") ;;
.netrc )
    l_mask='0177'; l_change="u-x,go-rwx"; file_access_fix
    a_netrc_warn+=("    - File: \"\$l_hdfilename\" exists") ;;
.bash_history )
    l_mask='0177'; l_change="u-x,go-rwx"; file_access_fix ;;
* )
    l_mask='0133'; l_change="u-x,go-wx"; file_access_fix ;;
esac
done <<(stat -Lc '%#a %U %G' \"\$l_hdfilename\")
done <<(find \"\$l_home\" -xdev -type f -name '*' -print0)
fi
[ \"\${#a_dot_file[@]}\" -gt 0 ] && a_output2+=(" - User: \"\$l_user\" Home
Directory: \"\$l_home\" \"\${a_dot_file[@]}")
[ \"\${#a_netrc_warn[@]}\" -gt 0 ] && a_output3+=(" - User: \"\$l_user\"
Home Directory: \"\$l_home\" \"\${a_netrc_warn[@]}")
done <<< \"$(printf '%s\\n' \"\${a_user_and_home[@]}\") \"
[ \"\${#a_output3[@]}\" -gt 0 ] && printf '%s\\n' \" \" \" ** WARNING **\"
\"${a_output3[@]}\" \" \"
[ \"\${#a_output2[@]}\" -gt 0 ] && printf '%s\\n' \" \" \"\${a_output2[@]}\"
}
```

## References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

**MITRE ATT&CK Mappings:**

| Techniques / Sub-techniques                                    | Tactics | Mitigations |
|----------------------------------------------------------------|---------|-------------|
| T1222, T1222.001,<br>T1222.002, T1552,<br>T1552.003, T1552.004 | TA0005  | M1022       |



### *7.2.11 Ensure all files and directories in the local interactive user home directory are group-owned by a group that the user is a member of (Automated)*

#### **Profile Applicability:**

- STIG

#### **Description:**

The operating system must be configured so that all files and directories contained in local interactive user home directories are group-owned by a group of which the home directory owner is a member.

#### **Rationale:**

If a local interactive user's files are group-owned by a group of which the user is not a member, unintended users may be able to access them.

#### **Audit:**

Verify all files and directories in a local interactive user home directory are group-owned by a group that the user is a member of.

Check the group owner of all files and directories in a local interactive user's home directory with the following command:

Note: The example will be for the user "smithj", who has a home directory of "/home/smithj".

```
# ls -lLR /<home directory>/<users home directory>/  
-rw-r--r-- 1 smithj smithj 18 Mar 5 17:06 file1  
-rw-r--r-- 1 smithj smithj 193 Mar 5 17:06 file2  
-rw-r--r-- 1 smithj sa 231 Mar 5 17:06 file3
```

If any files found with a group-owner different from the home directory user private group, check to see if the user is a member of that group with the following command:

```
# grep smithj /etc/group  
sa:x:100:juan,shelley,bob,smithj  
smithj:x:521:smithj
```

If any files or directories are group owned by a group that the directory owner is not a member of, this is a finding.

#### **Remediation:**

Change the group of a local interactive user's files and directories to a group that the interactive user is a member. To change the group owner of a local interactive user's files and directories, use the following command:

Note: The example will be for the user smithj, who has a home directory of "/home/smithj" and is a member of the users group.

```
# chgrp smithj /home/smithj/<file or directory>
```

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version 1, Release: 3 Benchmark Date: 23 Jul 2021

Vul ID: V-244532  
Rule ID: SV-244532r743845  
STIG ID: RHEL-08-010741  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |   |   |   |
| v7               | <b>14.6 Protect Information through Access Control Lists</b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## 7.2.12 Ensure all files and directories in a local interactive user home directory are mode 0750 or more restrictive (Automated)

### Profile Applicability:

- STIG

### Description:

All local interactive user home directory files must have mode "0750" or less permissive.

### Rationale:

Excessive permissions on local interactive user home directories may allow unauthorized access to user files by other users.

### Audit:

Verify all files and directories contained in a local interactive user home directory, excluding local initialization files, have a mode of "0750".

Files that begin with a "." are excluded from this requirement.

Note: The example will be for the user "smithj", who has a home directory of "/home/smithj".

```
# ls -lLR /home/smithj
-rwxr-x--- 1 smithj smithj 18 Mar 5 17:06 file1
-rwxr----- 1 smithj smithj 193 Mar 5 17:06 file2
-rw-r-x--- 1 smithj smithj 231 Mar 5 17:06 file3
```

If any files or directories are found with a mode more permissive than "0750", this is a finding.

### Remediation:

Set the mode on files and directories in the local interactive user home directory with the following command:

Note: The example will be for the user smithj, who has a home directory of "/home/smithj" and is a member of the users group.

```
# chmod 0750 /home/smithj/<file or directory>
```

### References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-244531  
Rule ID: SV-244531r743842  
STIG ID: RHEL-08-010731  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## 7.2.13 Ensure all local initialization files are mode 0740 or more restrictive (Automated)

### Profile Applicability:

- STIG

### Description:

All local initialization files must have mode "0740" or less permissive.

### Rationale:

Local initialization files are used to configure the user's shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

### Audit:

Verify that all local initialization files have a mode of "0740" or less permissive with the following command:

Note: The example will be for the "smithj" user, who has a home directory of "/home/smithj".

```
# ls -al /home/smithj/.[^.]* | more
-rwxr-xr-x 1 smithj users 896 Mar 10 2011 .profile
-rwxr-xr-x 1 smithj users 497 Jan 6 2007 .login
-rwxr-xr-x 1 smithj users 886 Jan 6 2007 .something
```

If any local initialization files have a mode more permissive than "0740", this is a finding.

### Remediation:

Set the mode of the local initialization files to "0740" with the following command:

Note: The example will be for the smithj user, who has a home directory of "/home/smithj".

```
# chmod g-wx,o-rwx /home/smithj/.<INIT_FILE>
```

### References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230325  
Rule ID: SV-230325r917879  
STIG ID: RHEL-08-010770  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.3 <u>Configure Data Access Control Lists</u></b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |  |  |  |
| v7               | <b>14.6 <u>Protect Information through Access Control Lists</u></b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |

## 7.2.14 Ensure local interactive user home directories group-owner is their primary GID (Automated)

### Profile Applicability:

- STIG

### Description:

All local interactive user home directories must be group-owned by the home directory owner's primary group.

### Rationale:

If the Group Identifier (GID) of a local interactive user's home directory is not the same as the primary GID of the user, this would allow unauthorized access to the user's files, and users that share the same group may not be able to access files that they legitimately should.

### Audit:

Verify the assigned home directory of all local interactive users is group-owned by that user's primary GID with the following command:

Note: This may miss local interactive users that have been assigned a privileged UID. Evidence of interactive use may be obtained from a number of log files containing system logon information. The returned directory "/home/smithj" is used as an example.

```
# ls -ld $(awk -F: '($3>=1000)&&($7 !~ /nologin/){print $6}' /etc/passwd)
drwxr-x--- 2 smithj admin 4096 Jun 5 12:41 smithj
```

Check the user's primary group with the following command:

```
# grep $(grep smithj /etc/passwd | awk -F: '{print $4}') /etc/group
admin:x:250:smithj,jonesj,jacksons
```

If the user home directory referenced in "/etc/passwd" is not group-owned by that user's primary GID, this is a finding.

### Remediation:

Change the group owner of a local interactive user's home directory to the group found in "/etc/passwd". To change the group owner of a local interactive user's home directory, use the following command:

Note: The example will be for the user "smithj", who has a home directory of "/home/smithj", and has a primary group of users.

```
# chgrp users /home/smithj
```

## References:

1. NIST SP 800-53 Revision 5 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

GROUP ID: V-230322  
RULE ID: SV-230322r880717  
STIG ID: RHEL-08-010740  
SEVERITY: CAT II

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.3 Configure Data Access Control Lists</b><br>Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.                                                                                                                                                        |   |   |   |
| v7               | <b>14.6 Protect Information through Access Control Lists</b><br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. |  |  |  |



## 7.2.15 Ensure file executable search path statements do not share sensitive home directory information (Manual)

### Profile Applicability:

- STIG

### Description:

Executable search paths within the initialization files of all local interactive operating system users must only contain paths that resolve to the system default or the users home directory.

### Rationale:

The executable search path (typically the PATH environment variable) contains a list of directories for the shell to search to find executables. If this path includes the current working directory (other than the user's home directory), executables in these directories may be executed instead of system commands. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is interpreted as the current working directory. If deviations from the default system search path for the local interactive user are required, they must be documented with the Information System Security Officer (ISSO).

### Audit:

Verify that all local interactive user initialization file executable search path statements do not contain statements that will reference a working directory other than user home directories with the following commands:

```
# grep -i path /home/*/.*/.*  
  
/home/[localinteractiveuser]/.bash_profile:PATH=$PATH:$HOME/.local/bin:$HOME/  
bin  
/home/[localinteractiveuser]/.bash_profile:export PATH
```

If any local interactive user initialization files have executable search path statements that include directories outside of their home directory and is not documented with the ISSO as an operational requirement, this is a finding.

### Remediation:

Edit the local interactive user initialization files to change any PATH variable statements that reference directories other than their home directory.

If a local interactive user requires path variables to reference a directory owned by the application, it must be documented with the ISSO.

## References:

1. NIST SP 800-53 :: CM-6 b
2. NIST SP 800-53A :: CM-6.1 (iv)

## Additional Information:

Red Hat Enterprise Linux 8 Security Technical Implementation Guide  
Version: 1 Release: 14 Benchmark Date: 24 Apr 2024

Vul ID: V-230317  
Rule ID: SV-230317r792896  
STIG ID: RHEL-08-010690  
Severity: CAT II

## CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

# Appendix: Summary Table

| CIS Benchmark Recommendation |                                                                                                      | Set Correctly            |                          |
|------------------------------|------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                      | Yes                      | No                       |
| <b>1</b>                     | <b>Initial Setup</b>                                                                                 |                          |                          |
| <b>1.1</b>                   | <b>Filesystem</b>                                                                                    |                          |                          |
| <b>1.1.1</b>                 | <b>Configure Filesystem Kernel Modules</b>                                                           |                          |                          |
| 1.1.1.1                      | Ensure cramfs kernel module is not available (Automated)                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.2                      | Ensure freevxfs kernel module is not available (Automated)                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.3                      | Ensure hfs kernel module is not available (Automated)                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.4                      | Ensure hfsplus kernel module is not available (Automated)                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.5                      | Ensure jffs2 kernel module is not available (Automated)                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.6                      | Ensure overlayfs kernel module is not available (Automated)                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.7                      | Ensure squashfs kernel module is not available (Automated)                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.8                      | Ensure udf kernel module is not available (Automated)                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.9                      | Ensure usb-storage kernel module is not available (Automated)                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.10                     | Ensure unused filesystems kernel modules are not available (Manual)                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.11                     | Ensure the operating system disables the ability to load the firewire-core kernel module (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.12                     | Ensure a camera is not installed (Automated)                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.1.2</b>                 | <b>Configure Filesystem Partitions</b>                                                               |                          |                          |

| CIS Benchmark Recommendation |                                                                                                                                 | Set Correctly            |                          |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                 | Yes                      | No                       |
| <b>1.1.2.1</b>               | <b>Configure /tmp</b>                                                                                                           |                          |                          |
| 1.1.2.1.1                    | Ensure /tmp is a separate partition (Automated)                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.2                    | Ensure nodev option set on /tmp partition (Automated)                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.3                    | Ensure nosuid option set on /tmp partition (Automated)                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.4                    | Ensure noexec option set on /tmp partition (Automated)                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.1.2.2</b>               | <b>Configure /dev/shm</b>                                                                                                       |                          |                          |
| 1.1.2.2.1                    | Ensure /dev/shm is a separate partition (Automated)                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.2                    | Ensure nodev option set on /dev/shm partition (Automated)                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.3                    | Ensure nosuid option set on /dev/shm partition (Automated)                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.4                    | Ensure noexec option set on /dev/shm partition (Automated)                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.1.2.3</b>               | <b>Configure /home</b>                                                                                                          |                          |                          |
| 1.1.2.3.1                    | Ensure separate partition exists for /home (Automated)                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.2                    | Ensure nodev option set on /home partition (Automated)                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.3                    | Ensure nosuid option set on /home partition (Automated)                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.4                    | Ensure a separate file system/partition has been created for non-privileged local interactive user home directories (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.5                    | Ensure file systems that contain user home directories are mounted with the nosuid option (Automated)                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.6                    | Ensure file systems that contain user home directories are mounted with the "noexec" option (Automated)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.1.2.4</b>               | <b>Configure /var</b>                                                                                                           |                          |                          |

| CIS Benchmark Recommendation |                                                                  | Set Correctly            |                          |
|------------------------------|------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                  | Yes                      | No                       |
| 1.1.2.4.1                    | Ensure separate partition exists for /var (Automated)            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.4.2                    | Ensure nodev option set on /var partition (Automated)            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.4.3                    | Ensure nosuid option set on /var partition (Automated)           | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.1.2.5</b>               | <b>Configure /var/tmp</b>                                        |                          |                          |
| 1.1.2.5.1                    | Ensure separate partition exists for /var/tmp (Automated)        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.2                    | Ensure nodev option set on /var/tmp partition (Automated)        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.3                    | Ensure nosuid option set on /var/tmp partition (Automated)       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.4                    | Ensure noexec option set on /var/tmp partition (Automated)       | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.1.2.6</b>               | <b>Configure /var/log</b>                                        |                          |                          |
| 1.1.2.6.1                    | Ensure separate partition exists for /var/log (Automated)        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.2                    | Ensure nodev option set on /var/log partition (Automated)        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.3                    | Ensure nosuid option set on /var/log partition (Automated)       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.4                    | Ensure noexec option set on /var/log partition (Automated)       | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.1.2.7</b>               | <b>Configure /var/log/audit</b>                                  |                          |                          |
| 1.1.2.7.1                    | Ensure separate partition exists for /var/log/audit (Automated)  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.2                    | Ensure nodev option set on /var/log/audit partition (Automated)  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.3                    | Ensure nosuid option set on /var/log/audit partition (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                 | Set Correctly            |                          |
|------------------------------|-------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                 | Yes                      | No                       |
| 1.1.2.7.4                    | Ensure noexec option set on /var/log/audit partition (Automated)                                | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.1.2.8</b>               | <b>Configure /boot</b>                                                                          |                          |                          |
| 1.1.2.8.1                    | Ensure the "/boot" directory is mounted with the "nosuid" option (Automated)                    | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.1.2.9</b>               | <b>Configure /boot/efi</b>                                                                      |                          |                          |
| 1.1.2.9.1                    | Ensure the "/boot/efi" directory is mounted with the "nosuid" option (Automated)                | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.1.2.10</b>              | <b>Configure nfs filesystems</b>                                                                |                          |                          |
| 1.1.2.10.1                   | Ensure file systems that are being NFS-imported are mounted with the "nodev" option (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.10.2                   | Ensure file systems being imported via NFS are mounted with the "nosuid" option (Automated)     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.10.3                   | Ensure file systems being imported via NFS are mounted with the "noexec" option (Automated)     | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.1.2.11</b>              | <b>Configure removable media partitions</b>                                                     |                          |                          |
| 1.1.2.11.1                   | Ensure nodev option set on removable media partitions (Manual)                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.11.2                   | Ensure nosuid option set on removable media partitions (Manual)                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.11.3                   | Ensure noexec option set on removable media partitions (Manual)                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.12                     | Ensure all non-root local partitions are mounted with the "nodev" option (Automated)            | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.1.3</b>                 | <b>Configure disk encryption</b>                                                                |                          |                          |
| 1.1.3.1                      | Ensure all information at rest is encrypted (Manual)                                            | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                                    | Set Correctly            |                          |
|------------------------------|--------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                    | Yes                      | No                       |
| <b>1.2</b>                   | <b>Package Management</b>                                                                                          |                          |                          |
| <b>1.2.1</b>                 | <b>Configure Package Repositories</b>                                                                              |                          |                          |
| 1.2.1.1                      | Ensure GPG keys are configured (Manual)                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.2                      | Ensure gpgcheck is globally activated (Automated)                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.3                      | Ensure repo_gpgcheck is globally activated (Manual)                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.4                      | Ensure package manager repositories are configured (Manual)                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.5                      | Ensure DNF is configured to perform a signature check on local packages (Automated)                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.6                      | Ensure cryptographic verification of vendor software packages (Manual)                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.2.2</b>                 | <b>Configure Package Updates</b>                                                                                   |                          |                          |
| 1.2.2.1                      | Ensure updates, patches, and additional security software are installed (Manual)                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2.2                      | Ensure vendor packaged system security patches and updates are installed (Manual)                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2.3                      | Ensure Operating System is a vendor-supported release (Manual)                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2.4                      | Ensure the operating system removes all software components after updated versions have been installed (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.3</b>                   | <b>Mandatory Access Control</b>                                                                                    |                          |                          |
| <b>1.3.1</b>                 | <b>Configure SELinux</b>                                                                                           |                          |                          |
| 1.3.1.1                      | Ensure SELinux is installed (Automated)                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.2                      | Ensure SELinux is not disabled in bootloader configuration (Automated)                                             | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                  | Set Correctly            |                          |
|------------------------------|--------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                  | Yes                      | No                       |
| 1.3.1.3                      | Ensure SELinux policy is configured (Automated)                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.4                      | Ensure the SELinux mode is not disabled (Automated)                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.5                      | Ensure the SELinux mode is enforcing (Automated)                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.6                      | Ensure no unconfined services exist (Manual)                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.7                      | Ensure the MCS Translation Service (mcstrans) is not installed (Automated)                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.8                      | Ensure the operating system has the policycoreutils package installed (Automated)                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.9                      | Ensure SETroubleshoot is not installed (Automated)                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.10                     | Ensure SELinux prevents nonprivileged users from executing privileged functions (Manual)         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.11                     | Ensure SELinux targeted policy is configured (Manual)                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.4</b>                   | <b>Configure Bootloader</b>                                                                      |                          |                          |
| 1.4.1                        | Ensure bootloader password is set (Automated)                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.2                        | Ensure access to bootloader config is configured (Automated)                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.3                        | Ensure the operating system requires authentication for rescue mode (Automated)                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.4                        | Ensure the operating system requires authentication upon booting into emergency mode (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.5                        | Ensure a unique name is set as the superusers account (BIOS) (Automated)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.6                        | Ensure a unique name is set as the superusers account (UEFI) (Automated)                         | <input type="checkbox"/> | <input type="checkbox"/> |



| CIS Benchmark Recommendation |                                                                                                                                               | Set Correctly            |                          |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                               | Yes                      | No                       |
| 1.4.7                        | Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed seven times within two seconds (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.8                        | Ensure GRUB 2 is configured to enable page poisoning to mitigate use-after-free vulnerabilities (Automated)                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.9                        | Ensure GRUB 2 is configured to enable poisoning of SLUB/SLAB objects to mitigate use-after-free vulnerabilities (Automated)                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.10                       | Ensure GRUB 2 is configured to disable vsyscalls (Automated)                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.5</b>                   | <b>Configure Additional Process Hardening</b>                                                                                                 |                          |                          |
| 1.5.1                        | Ensure address space layout randomization is enabled (Automated)                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.2                        | Ensure ptrace_scope is restricted (Automated)                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.3                        | Ensure core dump backtraces are disabled (Automated)                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.4                        | Ensure core dump storage is disabled (Automated)                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.5                        | Ensure the storing of core dumps is disabled (Automated)                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.6                        | Ensure the operating system is not configured to acquire save or process core dumps (Automated)                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.7                        | Ensure kernel core dumps are disabled unless needed (Automated)                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.8                        | Ensure the operating system enables hardening for the BPF JIT (Automated)                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.9                        | Ensure kernel page-table isolation is enabled (Automated)                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.10                       | Ensure the NX (no-execution) bit flag is set on the system (Automated)                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                                                 | Set Correctly            |                          |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                 | Yes                      | No                       |
| 1.5.11                       | Ensure the operating system disables the use of user namespaces (Automated)                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.12                       | Ensure kernel image loading is disabled (Automated)                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.13                       | Ensure the operating system is configured to enable DAC on symlinks (Automated)                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.14                       | Ensure the operating system is configured to boot to the command line (Manual)                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.15                       | Ensure the operating system is configured to enable DAC on hardlinks (Automated)                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.16                       | Ensure the operating system restricts exposed kernel pointer addresses access (Automated)                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.17                       | Ensure the operating system is configured to restrict access to the kernel message buffer (Automated)                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.18                       | Ensure the operating system disables core dumps for all users (Automated)                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.19                       | Ensure the operating system is configured to prevent kernel profiling by unprivileged users (Automated)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.20                       | Ensure the operating system restricts usage of ptrace to descendant processes (Automated)                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.21                       | Ensure the operating system prevents privilege escalation through the kernel by disabling access to the bpf syscall (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.22                       | Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed (Automated)                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.23                       | Ensure the operating system implements the Endpoint Security for Linux Threat Prevention tool (Automated)                       | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.6</b>                   | <b>Configure system wide crypto policy</b>                                                                                      |                          |                          |

| CIS Benchmark Recommendation |                                                                                                                   | Set Correctly            |                          |
|------------------------------|-------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                   | Yes                      | No                       |
| 1.6.1                        | Ensure system wide crypto policy is not set to legacy (Automated)                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.2                        | Ensure system wide crypto policy is not set in sshd configuration (Automated)                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.3                        | Ensure system wide crypto policy disables sha1 hash and signature support (Automated)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.4                        | Ensure system wide crypto policy disables macs less than 128 bits (Automated)                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.5                        | Ensure system wide crypto policy disables cbc for ssh (Automated)                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.6                        | Ensure system wide crypto policy disables chacha20-poly1305 for ssh (Manual)                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.7                        | Ensure system wide crypto policy disables EtM for ssh (Manual)                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.8                        | Ensure system-wide crypto policy is FIPS (Automated)                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.9                        | Ensure PKI-based authentication has valid certificates (Manual)                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.10                       | Ensure system-wide crypto policies are in effect (Automated)                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.11                       | Ensure the operating system implements certificate status checking for multifactor authentication (Automated)     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.12                       | Ensure the OpenSSL library is configured to use only ciphers employing FIPS 140-2-approved algorithms (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.13                       | Ensure the OpenSSL library is configured to use only DoD-approved TLS encryption (Automated)                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.14                       | Ensure the GnuTLS library is configured to only allow DoD-approved SSL/TLS Versions (Automated)                   | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                                                                                                 | Set Correctly            |                          |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                                                                 | Yes                      | No                       |
| <b>1.7</b>                   | <b>Configure Command Line Warning Banners</b>                                                                                                                                   |                          |                          |
| 1.7.1                        | Ensure message of the day is configured properly (Automated)                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.2                        | Ensure local login warning banner is configured properly (Automated)                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.3                        | Ensure remote login warning banner is configured properly (Automated)                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.4                        | Ensure access to /etc/motd is configured (Automated)                                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.5                        | Ensure access to /etc/issue is configured (Automated)                                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.6                        | Ensure access to /etc/issue.net is configured (Automated)                                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.7                        | Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a command line user logon (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.8</b>                   | <b>Configure GNOME Display Manager</b>                                                                                                                                          |                          |                          |
| 1.8.1                        | Ensure GNOME Display Manager is removed (Automated)                                                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.2                        | Ensure GDM login banner is configured (Automated)                                                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.3                        | Ensure GDM disable-user-list option is enabled (Automated)                                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.4                        | Ensure GDM screen locks when the user is idle (Automated)                                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.5                        | Ensure GDM screen locks cannot be overridden (Automated)                                                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.6                        | Ensure GDM automatic mounting of removable media is disabled (Automated)                                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                                                                      | Set Correctly            |                          |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                                      | Yes                      | No                       |
| 1.8.7                        | Ensure GDM disabling automatic mounting of removable media is not overridden (Automated)                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.8                        | Ensure the operating system does not allow an unattended or automatic logon to the system via a graphical user interface (Automated)                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.9                        | Ensure GDM autorun-never is enabled (Automated)                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.10                       | Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed when using a graphical user interface (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.11                       | Ensure GDM autorun-never is not overridden (Automated)                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.12                       | Ensure the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated (Automated)                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.13                       | Ensure XDMCP is not enabled (Automated)                                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.14                       | Ensure the operating system disables the user logon list for graphical user interfaces (Automated)                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.15                       | Ensure GDM login banner displays the Mandatory DoD Notice and Consent Banner (Manual)                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.16                       | Ensure the operating system prevents users from overriding the session idle-delay setting for the graphical user interface (Automated)               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.17                       | Ensure the operating system prevents users from overriding the screensaver lock-enabled setting for the graphical user interface (Automated)         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.18                       | Ensure the operating system initiates a session lock for all connection types using smartcard when the smartcard is removed (Manual)                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.19                       | Ensure the operating system enables a user's session lock until that user re-establishes access (Automated)                                          | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                                                 | Set Correctly            |                          |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                 | Yes                      | No                       |
| 1.9                          | Ensure the "tmux" package installed (Automated)                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.10                         | Ensure the system has the packages required to enable the hardware random number generator entropy gatherer service (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.11                         | Ensure the mailx package is installed (Automated)                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.12                         | Ensure the operating system accepts PIV credentials (Automated)                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.13                         | Ensure the operating system has the packages required for multifactor authentication (Automated)                                | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>2</b>                     | <b>Services</b>                                                                                                                 |                          |                          |
| <b>2.1</b>                   | <b>Configure Server Services</b>                                                                                                |                          |                          |
| 2.1.1                        | Ensure autofs services are not in use (Automated)                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.2                        | Ensure avahi daemon services are not in use (Automated)                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.3                        | Ensure dhcp server services are not in use (Automated)                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4                        | Ensure dns server services are not in use (Automated)                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.5                        | Ensure dnsmasq services are not in use (Automated)                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.6                        | Ensure ftp server services are not in use (Automated)                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.7                        | Ensure message access server services are not in use (Automated)                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.8                        | Ensure network file system services are not in use (Automated)                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.9                        | Ensure nis server services are not in use (Automated)                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.10                       | Ensure print server services are not in use (Automated)                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.11                       | Ensure rpcbind services are not in use (Automated)                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                               | Set Correctly            |                          |
|------------------------------|-----------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                               | Yes                      | No                       |
| 2.1.12                       | Ensure rsync services are not in use (Automated)                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.13                       | Ensure samba file server services are not in use (Automated)                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.14                       | Ensure snmp services are not in use (Automated)                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.15                       | Ensure telnet server services are not in use (Automated)                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.16                       | Ensure tftp server services are not in use (Automated)                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.17                       | Ensure web proxy server services are not in use (Automated)                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.18                       | Ensure web server services are not in use (Automated)                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.19                       | Ensure xinetd services are not in use (Automated)                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.20                       | Ensure X window server services are not in use (Automated)                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.21                       | Ensure only approved services are listening on a network interface (Manual)                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.22                       | Ensure automated bug reporting tools are not installed (Automated)                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.23                       | Ensure mail transfer agents are configured for local-only mode (Automated)                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.24                       | Ensure the sendmail package is not installed (Automated)                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.25                       | Ensure the rsh-server package is not installed (Automated)                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.26                       | Ensure system daemons are prevented from using Kerberos for authentication (Automated)        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.27                       | Ensure the operating system is configured to mask the debug-shell systemd service (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                                   | Set Correctly            |                          |
|------------------------------|-------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                   | Yes                      | No                       |
| 2.1.28                       | Ensure the gssproxy package has not been installed on the system (Automated)                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.29                       | Ensure the iprutils package has not been installed on the system (Automated)                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.30                       | Ensure the krb5-server package has not been installed on the system (Automated)                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.31                       | Ensure a TFTP server has not been installed on the system (Automated)                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.32                       | Ensure the tuned package has not been installed on the system (Automated)                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.33                       | Ensure the operating system has enabled the hardware random number generator entropy gatherer service (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.34                       | Ensure the operating system is configured to prevent unrestricted mail relaying (Automated)                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.35                       | Ensure the TFTP daemon is configured to operate in secure mode (Automated)                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>2.2</b>                   | <b>Configure Client Services</b>                                                                                  |                          |                          |
| 2.2.1                        | Ensure ftp client is not installed (Automated)                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.2                        | Ensure ldap client is not installed (Automated)                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.3                        | Ensure nis client is not installed (Automated)                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.4                        | Ensure telnet client is not installed (Automated)                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.5                        | Ensure tftp client is not installed (Automated)                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.6                        | Ensure krb5-workstation is not installed (Automated)                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>2.3</b>                   | <b>Configure Time Synchronization</b>                                                                             |                          |                          |
| 2.3.1                        | Ensure time synchronization is in use (Automated)                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |



| CIS Benchmark Recommendation |                                                                                                                                             | Set Correctly            |                          |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                             | Yes                      | No                       |
| 2.3.2                        | Ensure chrony is configured (Automated)                                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.3                        | Ensure chrony is not run as the root user (Automated)                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.4                        | Ensure the operating system is securely comparing internal information system clocks at least every 24 hours with an NTP server (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.5                        | Ensure the operating system disables network management of the chrony daemon (Automated)                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.6                        | Ensure the operating system disables the chrony daemon from acting as a server (Automated)                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>2.4</b>                   | <b>Job Schedulers</b>                                                                                                                       |                          |                          |
| <b>2.4.1</b>                 | <b>Configure cron</b>                                                                                                                       |                          |                          |
| 2.4.1.1                      | Ensure cron daemon is enabled and active (Automated)                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.2                      | Ensure permissions on /etc/crontab are configured (Automated)                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.3                      | Ensure permissions on /etc/cron.hourly are configured (Automated)                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.4                      | Ensure permissions on /etc/cron.daily are configured (Automated)                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.5                      | Ensure permissions on /etc/cron.weekly are configured (Automated)                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.6                      | Ensure permissions on /etc/cron.monthly are configured (Automated)                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.7                      | Ensure permissions on /etc/cron.d are configured (Automated)                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.8                      | Ensure crontab is restricted to authorized users (Automated)                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>2.4.2</b>                 | <b>Configure at</b>                                                                                                                         |                          |                          |

| CIS Benchmark Recommendation |                                                                                            | Set Correctly            |                          |
|------------------------------|--------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                            | Yes                      | No                       |
| 2.4.2.1                      | Ensure at is restricted to authorized users (Automated)                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>2.5</b>                   | <b>Configure USBGuard</b>                                                                  |                          |                          |
| 2.5.1                        | Ensure USBGuard is installed on the operating system (Automated)                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5.2                        | Ensure USBGuard has a policy configured (Manual)                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5.3                        | Ensure the operating system enables Linux audit logging of the USBGuard daemon (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5.4                        | Ensure the usbguard service is enabled and active (Automated)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>2.6</b>                   | <b>Configure fapolicyd</b>                                                                 |                          |                          |
| 2.6.1                        | Ensure fapolicyd is installed (Automated)                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.6.2                        | Ensure fapolicyd employs a deny-all, permit-by-exception policy (Automated)                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.6.3                        | Ensure fapolicyd is enabled and running (Automated)                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>3</b>                     | <b>Network</b>                                                                             |                          |                          |
| <b>3.1</b>                   | <b>Configure Network Devices</b>                                                           |                          |                          |
| 3.1.1                        | Ensure IPv6 status is identified (Manual)                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1.2                        | Ensure wireless interfaces are disabled (Automated)                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1.3                        | Ensure bluetooth services are not in use (Automated)                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1.4                        | Ensure network interfaces are not in promiscuous mode (Manual)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>3.2</b>                   | <b>Configure Network Kernel Modules</b>                                                    |                          |                          |
| 3.2.1                        | Ensure dccp kernel module is not available (Automated)                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.2                        | Ensure tipc kernel module is not available (Automated)                                     | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                | Set Correctly            |                          |
|------------------------------|----------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                | Yes                      | No                       |
| 3.2.3                        | Ensure rds kernel module is not available (Automated)          | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.4                        | Ensure sctp kernel module is not available (Automated)         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.5                        | Ensure atm kernel module is not available (Automated)          | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.6                        | Ensure bluetooth kernel module is not available (Automated)    | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.7                        | Ensure can kernel module is not available (Automated)          | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>3.3</b>                   | <b>Configure Network Kernel Parameters</b>                     |                          |                          |
| 3.3.1                        | Ensure ip forwarding is disabled (Automated)                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.2                        | Ensure packet redirect sending is disabled (Automated)         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.3                        | Ensure bogus icmp responses are ignored (Automated)            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.4                        | Ensure broadcast icmp requests are ignored (Automated)         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.5                        | Ensure icmp redirects are not accepted (Automated)             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.6                        | Ensure secure icmp redirects are not accepted (Automated)      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.7                        | Ensure reverse path filtering is enabled (Automated)           | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.8                        | Ensure source routed packets are not accepted (Automated)      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.9                        | Ensure suspicious packets are logged (Automated)               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.10                       | Ensure tcp syn cookies is enabled (Automated)                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.11                       | Ensure ipv6 router advertisements are not accepted (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.12                       | Ensure net.ipv4.conf.all.forwarding is disabled (Automated)    | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                                                     | Set Correctly            |                          |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                     | Yes                      | No                       |
| 3.4                          | Ensure at least two name servers are configured if using DNS resolution (Automated)                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>4</b>                     | <b>Host Based Firewall</b>                                                                                                          |                          |                          |
| <b>4.1</b>                   | <b>Configure a firewall utility</b>                                                                                                 |                          |                          |
| <b>4.1.1</b>                 | <b>Configure firewall rules</b>                                                                                                     |                          |                          |
| 4.1.1.1                      | Ensure nftables base chains exist (Automated)                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.2                      | Ensure host based firewall loopback traffic is configured (Automated)                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.3                      | Ensure firewalld drops unnecessary services and ports (Manual)                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.4                      | Ensure nftables established connections are configured (Manual)                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.5                      | Ensure nftables default deny firewall policy (Automated)                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2                        | Ensure the firewall is configured to remove unnecessary use of functions, ports, protocols, and/or services (Manual)                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.3                        | Ensure firewalld service is enabled and running (Automated)                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.4                        | Ensure nftables is installed (Automated)                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.5                        | Ensure a single firewall configuration utility is in use (Automated)                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.6                        | Ensure "nftables" is configured to allow rate limits on any connection to the system (Automated)                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.7                        | Ensure "firewalld" is installed (Automated)                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.8                        | Ensure "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                    | Set Correctly            |                          |
|------------------------------|------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                    | Yes                      | No                       |
| <b>5</b>                     | <b>Access Control</b>                                                              |                          |                          |
| <b>5.1</b>                   | <b>Configure SSH Server</b>                                                        |                          |                          |
| 5.1.1                        | Ensure openssh-server is installed (Automated)                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2                        | Ensure permissions on /etc/ssh/sshd_config are configured (Automated)              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3                        | Ensure permissions on SSH private host key files are configured (Automated)        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.4                        | Ensure permissions on SSH public host key files are configured (Automated)         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.5                        | Ensure sshd access is configured (Automated)                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.6                        | Ensure sshd Banner is configured (Automated)                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.7                        | Ensure sshd Ciphers are configured (Automated)                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.8                        | Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.9                        | Ensure sshd DisableForwarding is enabled (Automated)                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.10                       | Ensure sshd GSSAPIAuthentication is disabled (Automated)                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.11                       | Ensure sshd HostbasedAuthentication is disabled (Automated)                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.12                       | Ensure sshd IgnoreRhosts is enabled (Automated)                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.13                       | Ensure sshd KexAlgorithms is configured (Automated)                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.14                       | Ensure sshd LoginGraceTime is configured (Automated)                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.15                       | Ensure sshd LogLevel is configured (Automated)                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.16                       | Ensure sshd MACs are configured (Automated)                                        | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                              | Set Correctly            |                          |
|------------------------------|--------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                              | Yes                      | No                       |
| 5.1.17                       | Ensure sshd MaxAuthTries is configured (Automated)                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.18                       | Ensure sshd MaxSessions is configured (Automated)                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.19                       | Ensure sshd MaxStartups is configured (Automated)                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.20                       | Ensure sshd PermitEmptyPasswords is disabled (Automated)                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.21                       | Ensure sshd PermitRootLogin is disabled (Automated)                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.22                       | Ensure sshd PermitUserEnvironment is disabled (Automated)                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.23                       | Ensure sshd UsePAM is enabled (Automated)                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.24                       | Ensure sshd private key files have a passcode (Manual)                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.25                       | Ensure sshd X11Forwarding is disabled (Automated)                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.26                       | Ensure sshd ClientAliveInterval is configured (Automated)                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.27                       | Ensure sshd ClientAliveCountMax is configured (Automated)                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.28                       | Ensure the SSH server is configured to use only MACs employing FIPS 140-2-approved algorithms (Automated)    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.29                       | Ensure the SSH server is configured to use only ciphers employing FIPS 140-2-approved algorithms (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.30                       | Ensure sshd is configured to use only FIPS-validated key exchange algorithms (Automated)                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.31                       | Ensure the SSH server uses strong entropy (Automated)                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.32                       | Ensure sshd StrictModes is enabled (Automated)                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.33                       | Ensure sshd Banner is configured to display the Standard Mandatory DoD Notice and Consent Banner (Manual)    | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                                           | Set Correctly            |                          |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                           | Yes                      | No                       |
| 5.1.34                       | Ensure sshd IgnoreUserKnownHosts is enabled (Automated)                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.35                       | Ensure sshd X11UseLocalhost is enabled (Automated)                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.36                       | Ensure sshd KerberosAuthentication is disabled (Automated)                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.37                       | Ensure sshd RekeyLimit is configured (Automated)                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.38                       | Ensure sshd PrintLastLog is enabled (Automated)                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.39                       | Ensure SSH is loaded and active (Automated)                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5.2</b>                   | <b>Configure privilege escalation</b>                                                                                     |                          |                          |
| 5.2.1                        | Ensure sudo is installed (Automated)                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2                        | Ensure the sudoers file has the default include directory (Automated)                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3                        | Ensure sudo commands use pty (Automated)                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4                        | Ensure sudo log file exists (Automated)                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.5                        | Ensure users must provide password for escalation (Automated)                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.6                        | Ensure the sudoers file restricts sudo access to authorized personnel (Automated)                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.7                        | Ensure re-authentication for privilege escalation is not disabled globally (Automated)                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.8                        | Ensure the sudoers security policy is configured to use the invoking user's password for privilege escalation (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.9                        | Ensure sudo timestamp_timeout is configured (Automated)                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                           | Set Correctly            |                          |
|------------------------------|---------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                           | Yes                      | No                       |
| 5.2.10                       | Ensure access to the su command is restricted (Automated)                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.11                       | Ensure pam_succeed_if does not exist in /etc/pam.d/sudo (Automated)       | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5.3</b>                   | <b>Pluggable Authentication Modules</b>                                   |                          |                          |
| <b>5.3.1</b>                 | <b>Configure PAM software packages</b>                                    |                          |                          |
| 5.3.1.1                      | Ensure latest version of pam is installed (Automated)                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.1.2                      | Ensure latest version of authselect is installed (Automated)              | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5.3.2</b>                 | <b>Configure authselect</b>                                               |                          |                          |
| 5.3.2.1                      | Ensure active authselect profile includes pam modules (Automated)         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.2                      | Ensure pam_faillock module is enabled (Automated)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.3                      | Ensure pam_pwquality module is enabled (Automated)                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.4                      | Ensure pam_pwhistory module is enabled (Automated)                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.5                      | Ensure pam_unix module is enabled (Automated)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5.3.3</b>                 | <b>Configure PAM Arguments</b>                                            |                          |                          |
| <b>5.3.3.1</b>               | <b>Configure pam_faillock module</b>                                      |                          |                          |
| 5.3.3.1.1                    | Ensure password failed attempts lockout is configured (Automated)         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.2                    | Ensure password unlock time is configured (Automated)                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.3                    | Ensure password failed attempts lockout includes root account (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.4                    | Ensure deny is configured on the pam_faillock module (Automated)          | <input type="checkbox"/> | <input type="checkbox"/> |



| CIS Benchmark Recommendation |                                                                                                            | Set Correctly            |                          |
|------------------------------|------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                            | Yes                      | No                       |
| 5.3.3.1.5                    | Ensure deny is configured in /etc/security/faillock.conf (Automated)                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.6                    | Ensure fail_interval is configured on the pam_faillock module (Automated)                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.7                    | Ensure fail_interval is configured in /etc/security/faillock.conf (Automated)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.8                    | Ensure unlock_time is configured on the pam_faillock module (Automated)                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.9                    | Ensure unlock_time is configured in /etc/security/faillock.conf (Automated)                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.10                   | Ensure dir is configured on the pam_faillock module (Automated)                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.11                   | Ensure dir is configured in /etc/security/faillock.conf (Automated)                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.12                   | Ensure silent is set on the pam_faillock module (Automated)                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.13                   | Ensure silent is set in /etc/security/faillock.conf (Automated)                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.14                   | Ensure audit is set on the pam_faillock module (Automated)                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.15                   | Ensure audit is set in /etc/security/faillock.conf (Automated)                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.16                   | Ensure even_deny_root is set on the pam_faillock module (Automated)                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.17                   | Ensure even_deny_root is set in /etc/security/faillock.conf (Automated)                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.18                   | Ensure the use of a non-default faillock tally directory while SELinux enforces a targeted policy (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                                                       | Set Correctly            |                          |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                       | Yes                      | No                       |
| 5.3.3.1.19                   | Ensure the use of a non-default faillock tally directory on the pam_faillock module while SELinux enforces a targeted policy (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5.3.3.2</b>               | <b>Configure pam_pwquality module</b>                                                                                                 |                          |                          |
| 5.3.3.2.1                    | Ensure password number of changed characters is configured (Automated)                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.2                    | Ensure password length is configured (Automated)                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.3                    | Ensure password complexity is configured (Manual)                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.4                    | Ensure password same consecutive characters is configured (Automated)                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.5                    | Ensure password maximum sequential characters is configured (Automated)                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.6                    | Ensure password dictionary check is enabled (Automated)                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.7                    | Ensure password quality is enforced for the root user (Automated)                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.8                    | Ensure the operating system enforces a minimum 15-character password length (Automated)                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.9                    | Ensure ucredit is configured in /etc/security/pwquality.conf (Automated)                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.10                   | Ensure lcredit is configured in /etc/security/pwquality.conf (Automated)                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.11                   | Ensure dcredit is configured in /etc/security/pwquality.conf (Automated)                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.12                   | Ensure ocredit is configured in /etc/security/pwquality.conf (Automated)                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.13                   | Ensure maxclassrepeat is configured in /etc/security/pwquality.conf (Automated)                                                       | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                   | Set Correctly            |                          |
|------------------------------|---------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                   | Yes                      | No                       |
| 5.3.3.2.14                   | Ensure minclass is configured in /etc/security/pwquality.conf (Automated)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.15                   | Ensure difok is configured in /etc/security/pwquality.conf (Automated)                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.16                   | Ensure dictcheck is configured (Automated)                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.17                   | Ensure retry is configured on the pam_pwquality module in /etc/pam.d/system-auth (Automated)      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.18                   | Ensure retry is configured on the pam_pwquality module in /etc/pam.d/password-auth (Automated)    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.19                   | Ensure retry is configured in /etc/security/pwquality.conf (Automated)                            | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5.3.3.3</b>               | <b>Configure pam_pwhistory module</b>                                                             |                          |                          |
| 5.3.3.3.1                    | Ensure password history remember is configured (Automated)                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.2                    | Ensure password history is enforced for the root user (Automated)                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.3                    | Ensure pam_pwhistory includes use_authok (Automated)                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.4                    | Ensure remember is configured on the pam_pwhistory module in /etc/pam.d/password-auth (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.5                    | Ensure remember is configured on the pam_pwhistory module in /etc/pam.d/system-auth (Automated)   | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5.3.3.4</b>               | <b>Configure pam_unix module</b>                                                                  |                          |                          |
| 5.3.3.4.1                    | Ensure pam_unix does not include nullok (Automated)                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.2                    | Ensure pam_unix does not include remember (Automated)                                             | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                                           | Set Correctly            |                          |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                           | Yes                      | No                       |
| 5.3.3.4.3                    | Ensure pam_unix includes a strong password hashing algorithm (Automated)                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.4                    | Ensure pam_unix includes use_authtok (Automated)                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.5                    | Ensure pam_unix includes a FIPS 140-2 approved hashing algorithm (Automated)                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5.3.3.5</b>               | <b>Configure pam_lastlog module</b>                                                                                       |                          |                          |
| 5.3.3.5.1                    | Ensure the date and time of the last successful account logon upon logon is displayed (Automated)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5.3.3.6</b>               | <b>Configure pam_sss module</b>                                                                                           |                          |                          |
| 5.3.3.6.1                    | Ensure the operating system uses multifactor authentication for local access to accounts (Automated)                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.6.2                    | Ensure SSSD prohibits the use of cached authentications after one day (Automated)                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.6.3                    | Ensure the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5.4</b>                   | <b>User Accounts and Environment</b>                                                                                      |                          |                          |
| <b>5.4.1</b>                 | <b>Configure shadow password suite parameters</b>                                                                         |                          |                          |
| 5.4.1.1                      | Ensure password expiration is configured (Automated)                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.2                      | Ensure minimum password days is configured (Automated)                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.3                      | Ensure password expiration warning days is configured (Automated)                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.4                      | Ensure strong password hashing algorithm is configured (Automated)                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.5                      | Ensure inactive password lock is configured (Automated)                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                               | Set Correctly            |                          |
|------------------------------|-----------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                               | Yes                      | No                       |
| 5.4.1.6                      | Ensure all users last password change date is in the past (Automated)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.7                      | Ensure passwords use FIPS 140-2 approved cryptographic hashing algorithm (Automated)          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.8                      | Ensure minimum number of hashing rounds is configured (Automated)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.9                      | Ensure existing passwords use FIPS 140-2 approved cryptographic hashing algorithm (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.10                     | Ensure temporary accounts have been provisioned with an expiration date of 72 hours (Manual)  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.11                     | Ensure fail_delay is configured (Automated)                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.12                     | Ensure pass_min_len is configured (Automated)                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.13                     | Ensure the maximum time period for existing passwords is restricted to 60 days (Automated)    | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5.4.2</b>                 | <b>Configure root and system accounts and environment</b>                                     |                          |                          |
| 5.4.2.1                      | Ensure root is the only UID 0 account (Automated)                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.2                      | Ensure root is the only GID 0 account (Automated)                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.3                      | Ensure group root is the only GID 0 group (Automated)                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.4                      | Ensure root account access is controlled (Automated)                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.5                      | Ensure root path integrity (Automated)                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.6                      | Ensure root user umask is configured (Automated)                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.7                      | Ensure system accounts do not have a valid login shell (Automated)                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.8                      | Ensure accounts without a valid login shell are locked (Automated)                            | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                                                                                      | Set Correctly            |                          |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                                                      | Yes                      | No                       |
| 5.4.2.9                      | Ensure all accounts on the system are assigned to an active system, application, or user account (Manual)                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5.4.3</b>                 | <b>Configure user default environment</b>                                                                                                                            |                          |                          |
| 5.4.3.1                      | Ensure nologin is not listed in /etc/shells (Automated)                                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.2                      | Ensure default user shell timeout is configured (Automated)                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.3                      | Ensure default user umask is configured (Automated)                                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.4                      | Ensure emergency accounts have been provisioned with an expiration date of 72 hours (Manual)                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.5                      | Ensure the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity (Automated)                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.6                      | Ensure the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.7                      | Ensure the operating system enforces a 60-day maximum password lifetime for new user accounts (Automated)                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.8                      | Ensure the umask default for installed shells is "077" (Automated)                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.9                      | Ensure the default umask for all local interactive users is "077" (Manual)                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.10                     | Ensure the operating system initiates a session lock after 15 minutes of inactivity (Automated)                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.11                     | Ensure the operating system prevents users from disabling the tmux terminal multiplexer (Automated)                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.12                     | Ensure the operating system's shell initialization file is configured to start each shell with the tmux terminal multiplexer (Automated)                             | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                               | Set Correctly            |                          |
|------------------------------|---------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                               | Yes                      | No                       |
| 5.4.3.13                     | Ensure the operating system enables the user to initiate a session lock (Automated)                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.14                     | Ensure the number of concurrent sessions is configured (Automated)                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.15                     | Ensure all local interactive users are assigned a home directory upon creation (Automated)                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.16                     | Ensure StopIdleSessionSec is configured (Automated)                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>6</b>                     | <b>Logging and Auditing</b>                                                                                   |                          |                          |
| <b>6.1</b>                   | <b>Configure Integrity Checking</b>                                                                           |                          |                          |
| 6.1.1                        | Ensure AIDE is installed (Automated)                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.2                        | Ensure filesystem integrity is regularly checked (Automated)                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.3                        | Ensure cryptographic mechanisms are used to protect the integrity of audit tools (Automated)                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.4                        | Ensure AIDE is configured to use cryptographic mechanisms to protect the integrity of audit tools (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.5                        | Ensure the file integrity tool is configured to verify ACLs (Manual)                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.6                        | Ensure the file integrity tool is configured to verify extended attributes (Manual)                           | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>6.2</b>                   | <b>System Logging</b>                                                                                         |                          |                          |
| <b>6.2.1</b>                 | <b>Configure journald</b>                                                                                     |                          |                          |
| <b>6.2.1.1</b>               | <b>Configure systemd-journald service</b>                                                                     |                          |                          |
| 6.2.1.1.1                    | Ensure journald service is enabled and active (Automated)                                                     | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                     | Set Correctly            |                          |
|------------------------------|---------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                     | Yes                      | No                       |
| 6.2.1.1.2                    | Ensure journald log file access is configured (Manual)              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.3                    | Ensure journald log file rotation is configured (Manual)            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.4                    | Ensure journald ForwardToSyslog is disabled (Automated)             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.5                    | Ensure journald Storage is configured (Automated)                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.6                    | Ensure journald Compress is configured (Automated)                  | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>6.2.1.2</b>               | <b>Configure systemd-journal-remote</b>                             |                          |                          |
| 6.2.1.2.1                    | Ensure systemd-journal-remote is installed (Automated)              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.2                    | Ensure systemd-journal-remote authentication is configured (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.3                    | Ensure systemd-journal-upload is enabled and active (Automated)     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.4                    | Ensure systemd-journal-remote service is not in use (Automated)     | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>6.2.2</b>                 | <b>Configure rsyslog</b>                                            |                          |                          |
| 6.2.2.1                      | Ensure rsyslog is installed (Automated)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.2                      | Ensure rsyslog service is enabled and active (Automated)            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.3                      | Ensure all remote access methods are monitored (Automated)          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.4                      | Ensure journald is configured to send logs to rsyslog (Automated)   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.5                      | Ensure rsyslog log file creation mode is configured (Automated)     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.6                      | Ensure rsyslog logging is configured (Manual)                       | <input type="checkbox"/> | <input type="checkbox"/> |



| CIS Benchmark Recommendation |                                                                                                                                          | Set Correctly            |                          |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                          | Yes                      | No                       |
| 6.2.2.7                      | Ensure rsyslog is configured to send logs to a remote log host (Manual)                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.8                      | Ensure rsyslog is not configured to receive logs from a remote client (Automated)                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.9                      | Ensure logrotate is configured (Manual)                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.10                     | Ensure rsyslog is configured to log cron events (Automated)                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.11                     | Ensure the rsyslog service is enabled and active (Automated)                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.12                     | Ensure the operating system has the packages required for encrypting offloaded audit logs (Automated)                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.13                     | Ensure the the operating system authenticates the remote logging server for off-loading audit logs (Automated)                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.14                     | Ensure the operating system encrypts audit records off-loaded onto a different system or media from the system being audited (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.15                     | Ensure the audit system off-loads audit records onto a different system or media from the system being audited (Automated)               | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>6.2.3</b>                 | <b>Configure Logfiles</b>                                                                                                                |                          |                          |
| 6.2.3.1                      | Ensure access to all logfiles has been configured (Automated)                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.2                      | Ensure /var/log/messages mode is configured (Automated)                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.3                      | Ensure /var/log/messages owner is configured (Automated)                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.4                      | Ensure /var/log/messages group owner is configured (Automated)                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                                                              | Set Correctly            |                          |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                              | Yes                      | No                       |
| 6.2.3.5                      | Ensure /var/log is mode is configured (Automated)                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.6                      | Ensure /var/log owner is configured (Automated)                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.7                      | Ensure /var/log group owner is configured (Automated)                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.8                      | Ensure administrators are notified if an audit processing failure occurs by modifying /etc/aliases (Automated)                               | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>6.3</b>                   | <b>System Auditing</b>                                                                                                                       |                          |                          |
| <b>6.3.1</b>                 | <b>Configure auditd Service</b>                                                                                                              |                          |                          |
| 6.3.1.1                      | Ensure auditd packages are installed (Automated)                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.2                      | Ensure auditing for processes that start prior to auditd is enabled (Automated)                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.3                      | Ensure audit_backlog_limit is sufficient (Automated)                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.4                      | Ensure auditd service is enabled and active (Automated)                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.5                      | Ensure the operating system allocates a sufficient audit_backlog_limit to capture processes that start prior to the audit daemon (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.6                      | Ensure the operating system's audit daemon is configured to include local events (Automated)                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.7                      | Ensure the operating system's audit daemon is configured to label all off-loaded audit logs (Automated)                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.8                      | Ensure the operating system's audit daemon is configured to resolve audit information before writing to disk (Automated)                     | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>6.3.2</b>                 | <b>Configure Data Retention</b>                                                                                                              |                          |                          |
| 6.3.2.1                      | Ensure audit log storage size is configured (Automated)                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.2                      | Ensure audit logs are not automatically deleted (Automated)                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                                                                                            | Set Correctly            |                          |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                                                            | Yes                      | No                       |
| 6.3.2.3                      | Ensure system is disabled when audit logs are full (Automated)                                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.4                      | Ensure system warns when audit logs are low on space (Automated)                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.5                      | Ensure the operating system allocates audit record storage capacity (Manual)                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.6                      | Ensure the SA and ISSO are notified in the event of an audit processing failure (Automated)                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.7                      | Ensure the operating system notifies the SA and ISSO when allocated audit record storage volume reaches 75 percent (Automated)                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.8                      | Ensure the operating system takes action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.9                      | Ensure the audit system is configured to take an appropriate action when the internal event queue is full (Automated)                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>6.3.3</b>                 | <b>Configure auditd Rules</b>                                                                                                                                              |                          |                          |
| 6.3.3.1                      | Ensure changes to system administration scope (sudoers) is collected (Automated)                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.2                      | Ensure actions as another user are always logged (Automated)                                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.3                      | Ensure events that modify the sudo log file are collected (Automated)                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.4                      | Ensure events that modify date and time information are collected (Automated)                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.5                      | Ensure events that modify the system's network environment are collected (Automated)                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                  | Set Correctly            |                          |
|------------------------------|--------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                  | Yes                      | No                       |
| 6.3.3.6                      | Ensure use of privileged commands are collected (Automated)                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.7                      | Ensure unsuccessful file access attempts are collected (Automated)                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.8                      | Ensure events that modify user/group information are collected (Automated)                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.9                      | Ensure discretionary access control permission modification events are collected (Automated)     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.10                     | Ensure successful file system mounts are collected (Automated)                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.11                     | Ensure session initiation information is collected (Automated)                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.12                     | Ensure login and logout events are collected (Automated)                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.13                     | Ensure file deletion events by users are collected (Automated)                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.14                     | Ensure events that modify the system's Mandatory Access Controls are collected (Automated)       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.15                     | Ensure successful and unsuccessful attempts to use the chcon command are collected (Automated)   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.16                     | Ensure successful and unsuccessful attempts to use the setfacl command are collected (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.17                     | Ensure successful and unsuccessful attempts to use the chacl command are collected (Automated)   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.18                     | Ensure successful and unsuccessful attempts to use the usermod command are collected (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.19                     | Ensure kernel module loading unloading and modification is collected (Automated)                 | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                              | Set Correctly            |                          |
|------------------------------|--------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                              | Yes                      | No                       |
| 6.3.3.20                     | Ensure the audit configuration is immutable (Automated)                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.21                     | Ensure the running and on disk configuration is the same (Manual)                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.22                     | Ensure successful and unsuccessful attempts to use the su command are collected (Automated)                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.23                     | Ensure successful and unsuccessful attempts to use the sudo command are collected (Automated)                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.24                     | Ensure successful and unsuccessful attempts to use the chsh command are collected (Automated)                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.25                     | Ensure successful and unsuccessful attempts to use the crontab command are collected (Automated)             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.26                     | Ensure successful and unsuccessful attempts to use the gpasswd command are collected (Automated)             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.27                     | Ensure successful and unsuccessful attempts to use the newgrp command are collected (Automated)              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.28                     | Ensure successful and unsuccessful attempts to use the pam_timestamp_check command are collected (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.29                     | Ensure successful and unsuccessful attempts to use the ssh-keysign command are collected (Automated)         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.30                     | Ensure successful and unsuccessful attempts to use the unix_chkpwd command are collected (Automated)         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.31                     | Ensure successful and unsuccessful attempts to use the setsebool command are collected (Automated)           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.32                     | Ensure successful and unsuccessful attempts to use the userhelper command are collected (Automated)          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.33                     | Ensure successful and unsuccessful attempts to use the setfiles command are collected (Automated)            | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                      | Set Correctly            |                          |
|------------------------------|------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                      | Yes                      | No                       |
| 6.3.3.34                     | Ensure successful and unsuccessful attempts to use the semanage command are collected (Automated)    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.35                     | Ensure successful and unsuccessful attempts to use the postqueue command are collected (Automated)   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.36                     | Ensure successful and unsuccessful attempts to use the postdrop command are collected (Automated)    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.37                     | Ensure successful and unsuccessful attempts to use the unix_update command are collected (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.38                     | Ensure successful and unsuccessful attempts to use the umount command are collected (Automated)      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.39                     | Ensure successful and unsuccessful attempts to use the mount command are collected (Automated)       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.40                     | Ensure successful and unsuccessful attempts to use the ssh-agent command are collected (Automated)   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.41                     | Ensure successful and unsuccessful attempts to use the passwd command are collected (Automated)      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.42                     | Ensure successful and unsuccessful attempts to use the chage command are collected (Automated)       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.43                     | Ensure the audit system prevents unauthorized changes to logon UIDs (Automated)                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.44                     | Ensure successful and unsuccessful modifications to the faillock file are collected (Automated)      | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>6.3.4</b>                 | <b>Configure auditd File Access</b>                                                                  |                          |                          |
| 6.3.4.1                      | Ensure the audit log file directory mode is configured (Automated)                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.2                      | Ensure audit log files mode is configured (Automated)                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.3                      | Ensure audit log files owner is configured (Automated)                                               | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                     | Set Correctly            |                          |
|------------------------------|-------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                     | Yes                      | No                       |
| 6.3.4.4                      | Ensure audit log files group owner is configured (Automated)                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.5                      | Ensure audit configuration files mode is configured (Automated)                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.6                      | Ensure audit configuration files owner is configured (Automated)                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.7                      | Ensure audit configuration files group owner is configured (Automated)              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.8                      | Ensure audit tools mode is configured (Automated)                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.9                      | Ensure audit tools owner is configured (Automated)                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.10                     | Ensure audit tools group owner is configured (Automated)                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.11                     | Ensure the audit logs are group-owned by root (Automated)                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.12                     | Ensure audit tools are mode 0755 or more restrictive (Automated)                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.13                     | Ensure the audit tools are owned by root (Automated)                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.14                     | Ensure audit tools are group owned by root (Automated)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.15                     | Ensure the audit log file directories are mode 0700 or more restrictive (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.16                     | Ensure the audit log file directory is owned by root (Automated)                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.17                     | Ensure audit log files group owner is root (Automated)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.18                     | Ensure audit log files are mode 0600 or more restrictive (Automated)                | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>7</b>                     | <b>System Maintenance</b>                                                           |                          |                          |

| CIS Benchmark Recommendation |                                                                               | Set Correctly            |                          |
|------------------------------|-------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                               | Yes                      | No                       |
| <b>7.1</b>                   | <b>System File Permissions</b>                                                |                          |                          |
| 7.1.1                        | Ensure permissions on /etc/passwd are configured (Automated)                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.2                        | Ensure permissions on /etc/passwd- are configured (Automated)                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.3                        | Ensure permissions on /etc/group are configured (Automated)                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.4                        | Ensure permissions on /etc/group- are configured (Automated)                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.5                        | Ensure permissions on /etc/shadow are configured (Automated)                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.6                        | Ensure permissions on /etc/shadow- are configured (Automated)                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.7                        | Ensure permissions on /etc/gshadow are configured (Automated)                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.8                        | Ensure permissions on /etc/gshadow- are configured (Automated)                | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.9                        | Ensure permissions on /etc/shells are configured (Automated)                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.10                       | Ensure permissions on /etc/security/opasswd are configured (Automated)        | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.11                       | Ensure world writable files and directories are secured (Automated)           | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.12                       | Ensure no files or directories without an owner and a group exist (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.13                       | Ensure SUID and SGID files are reviewed (Manual)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.14                       | Ensure there are no ".shosts" files on the operating system (Automated)       | <input type="checkbox"/> | <input type="checkbox"/> |



| CIS Benchmark Recommendation |                                                                                                                                       | Set Correctly            |                          |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                       | Yes                      | No                       |
| 7.1.15                       | Ensure there are no "shosts.equiv" files on the operating system (Automated)                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.16                       | Ensure system-wide shared library directories have mode 755 or less permissive (Automated)                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.17                       | Ensure system-wide shared library directories must be owned by root (Automated)                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.18                       | Ensure the system-wide shared library directories are group-owned by root or a system account (Automated)                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.19                       | Ensure world-writable directories owner is configured (Manual)                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.20                       | Ensure world-writable directories group-owner is configured (Manual)                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.21                       | Ensure local initialization files do not execute world-writable programs (Manual)                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.22                       | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are mode 0755 or more restrictive (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.23                       | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are owned by root (Automated)                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.24                       | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are group-owned by root (Automated)           | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.25                       | Ensure the system-wide shared library files are mode 0755 or more restrictive (Automated)                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.26                       | Ensure the system-wide shared library files are owned by root (Automated)                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.27                       | Ensure the system-wide shared library files are group-owned by root (Automated)                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>7.2</b>                   | <b>Local User and Group Settings</b>                                                                                                  |                          |                          |

| CIS Benchmark Recommendation |                                                                                                                                                   | Set Correctly            |                          |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                                   | Yes                      | No                       |
| 7.2.1                        | Ensure accounts in /etc/passwd use shadowed passwords (Automated)                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.2                        | Ensure /etc/shadow password fields are not empty (Automated)                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.3                        | Ensure all groups in /etc/passwd exist in /etc/group (Automated)                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.4                        | Ensure shadow group is empty (Automated)                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.5                        | Ensure no duplicate UIDs exist (Automated)                                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.6                        | Ensure no duplicate GIDs exist (Automated)                                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.7                        | Ensure no duplicate user names exist (Automated)                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.8                        | Ensure no duplicate group names exist (Automated)                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.9                        | Ensure local interactive user home directories are configured (Automated)                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.10                       | Ensure local interactive user dot files access is configured (Automated)                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.11                       | Ensure all files and directories in the local interactive user home directory are group-owned by a group that the user is a member of (Automated) | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.12                       | Ensure all files and directories in a local interactive user home directory are mode 0750 or more restrictive (Automated)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.13                       | Ensure all local initialization files are mode 0740 or more restrictive (Automated)                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.14                       | Ensure local interactive user home directories group-owner is their primary GID (Automated)                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.15                       | Ensure file executable search path statements do not share sensitive home directory information (Manual)                                          | <input type="checkbox"/> | <input type="checkbox"/> |



# Appendix: CIS Controls v7 IG 1 Mapped Recommendations

| Recommendation |                                                                                             | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                             | Yes                      | No                       |
| 1.1.2.1.3      | Ensure nosuid option set on /tmp partition                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.4      | Ensure noexec option set on /tmp partition                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.2      | Ensure nodev option set on /dev/shm partition                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.3      | Ensure nosuid option set on /dev/shm partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.4      | Ensure noexec option set on /dev/shm partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.1      | Ensure separate partition exists for /home                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.2      | Ensure nodev option set on /home partition                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.3      | Ensure nosuid option set on /home partition                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.5      | Ensure file systems that contain user home directories are mounted with the nosuid option   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.6      | Ensure file systems that contain user home directories are mounted with the "noexec" option | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.4.1      | Ensure separate partition exists for /var                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.4.2      | Ensure nodev option set on /var partition                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.4.3      | Ensure nosuid option set on /var partition                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.1      | Ensure separate partition exists for /var/tmp                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.2      | Ensure nodev option set on /var/tmp partition                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.3      | Ensure nosuid option set on /var/tmp partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.4      | Ensure noexec option set on /var/tmp partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.2      | Ensure nodev option set on /var/log partition                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.3      | Ensure nosuid option set on /var/log partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.4      | Ensure noexec option set on /var/log partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.2      | Ensure nodev option set on /var/log/audit partition                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.3      | Ensure nosuid option set on /var/log/audit partition                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.4      | Ensure noexec option set on /var/log/audit partition                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.8.1      | Ensure the "/boot" directory is mounted with the "nosuid" option                            | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                  | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                  | Yes                      | No                       |
| 1.1.2.9.1      | Ensure the <code>"/boot/efi"</code> directory is mounted with the <code>"nosuid"</code> option   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.10.1     | Ensure file systems that are being NFS-imported are mounted with the <code>"nodev"</code> option | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.10.2     | Ensure file systems being imported via NFS are mounted with the <code>"nosuid"</code> option     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.10.3     | Ensure file systems being imported via NFS are mounted with the <code>"noexec"</code> option     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.11.1     | Ensure <code>nodev</code> option set on removable media partitions                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.11.2     | Ensure <code>nosuid</code> option set on removable media partitions                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.11.3     | Ensure <code>noexec</code> option set on removable media partitions                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.12       | Ensure all non-root local partitions are mounted with the <code>"nodev"</code> option            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.1        | Ensure GPG keys are configured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.2        | Ensure <code>gpgcheck</code> is globally activated                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.3        | Ensure <code>repo_gpgcheck</code> is globally activated                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.4        | Ensure package manager repositories are configured                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.5        | Ensure DNF is configured to perform a signature check on local packages                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2.1        | Ensure updates, patches, and additional security software are installed                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2.2        | Ensure vendor packaged system security patches and updates are installed                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.1        | Ensure SELinux is installed                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.2        | Ensure SELinux is not disabled in bootloader configuration                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.3        | Ensure SELinux policy is configured                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.4        | Ensure the SELinux mode is not disabled                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.5        | Ensure the SELinux mode is enforcing                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.8        | Ensure the operating system has the <code>polycoreutils</code> package installed                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.9        | Ensure <code>SETroubleshoot</code> is not installed                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.10       | Ensure SELinux prevents nonprivileged users from executing privileged functions                  | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                  | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                  | Yes                      | No                       |
| 1.4.1          | Ensure bootloader password is set                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.2          | Ensure access to bootloader config is configured                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.13         | Ensure the operating system is configured to enable DAC on symlinks                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.15         | Ensure the operating system is configured to enable DAC on hardlinks                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.17         | Ensure the operating system is configured to restrict access to the kernel message buffer                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.19         | Ensure the operating system is configured to prevent kernel profiling by unprivileged users                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.21         | Ensure the operating system prevents privilege escalation through the kernel by disabling access to the bpf syscall              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.4          | Ensure access to /etc/motd is configured                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.5          | Ensure access to /etc/issue is configured                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.6          | Ensure access to /etc/issue.net is configured                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.4          | Ensure GDM screen locks when the user is idle                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.5          | Ensure GDM screen locks cannot be overridden                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.6          | Ensure GDM automatic mounting of removable media is disabled                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.7          | Ensure GDM disabling automatic mounting of removable media is not overridden                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.9          | Ensure GDM autorun-never is enabled                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.11         | Ensure GDM autorun-never is not overridden                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.12         | Ensure the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.16         | Ensure the operating system prevents users from overriding the session idle-delay setting for the graphical user interface       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.17         | Ensure the operating system prevents users from overriding the screensaver lock-enabled setting for the graphical user interface | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.19         | Ensure the operating system enables a user's session lock until that user re-establishes access                                  | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                             | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                             | Yes                      | No                       |
| 1.9            | Ensure the "tmux" package installed                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.1          | Ensure autofs services are not in use                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.15         | Ensure telnet server services are not in use                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.2          | Ensure ldap client is not installed                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.4          | Ensure telnet client is not installed                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.2        | Ensure permissions on /etc/crontab are configured                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.3        | Ensure permissions on /etc/cron.hourly are configured                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.4        | Ensure permissions on /etc/cron.daily are configured                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.5        | Ensure permissions on /etc/cron.weekly are configured                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.6        | Ensure permissions on /etc/cron.monthly are configured                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.7        | Ensure permissions on /etc/cron.d are configured                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.8        | Ensure crontab is restricted to authorized users                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.2.1        | Ensure at is restricted to authorized users                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5.3          | Ensure the operating system enables Linux audit logging of the USBGuard daemon                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.6.2          | Ensure fapolicyd employs a deny-all, permit-by-exception policy                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.6.3          | Ensure fapolicyd is enabled and running                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.9          | Ensure suspicious packets are logged                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.1        | Ensure nftables base chains exist                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.2        | Ensure host based firewall loopback traffic is configured                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.3        | Ensure firewalld drops unnecessary services and ports                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.4        | Ensure nftables established connections are configured                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.5        | Ensure nftables default deny firewall policy                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2          | Ensure the firewall is configured to remove unnecessary use of functions, ports, protocols, and/or services | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.3          | Ensure firewalld service is enabled and running                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.4          | Ensure nftables is installed                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.5          | Ensure a single firewall configuration utility is in use                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.6          | Ensure "nftables" is configured to allow rate limits on any connection to the system                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.7          | Ensure "firewalld" is installed                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                            | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                            | Yes                      | No                       |
| 4.1.8          | Ensure "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2          | Ensure permissions on /etc/ssh/sshd_config are configured                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3          | Ensure permissions on SSH private host key files are configured                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.4          | Ensure permissions on SSH public host key files are configured                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.5          | Ensure sshd access is configured                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.15         | Ensure sshd LogLevel is configured                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.21         | Ensure sshd PermitRootLogin is disabled                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.24         | Ensure sshd private key files have a passcode                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.26         | Ensure sshd ClientAliveInterval is configured                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.27         | Ensure sshd ClientAliveCountMax is configured                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1          | Ensure sudo is installed                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3          | Ensure sudo commands use pty                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.5          | Ensure users must provide password for escalation                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.6          | Ensure the sudoers file restricts sudo access to authorized personnel                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.7          | Ensure re-authentication for privilege escalation is not disabled globally                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.9          | Ensure sudo timestamp_timeout is configured                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.10         | Ensure access to the su command is restricted                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.11         | Ensure pam_succeed_if does not exist in /etc/pam.d/sudo                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.2        | Ensure root is the only GID 0 account                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.3        | Ensure group root is the only GID 0 group                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.4        | Ensure root account access is controlled                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.6        | Ensure root user umask is configured                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.7        | Ensure system accounts do not have a valid login shell                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.8        | Ensure accounts without a valid login shell are locked                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.2        | Ensure default user shell timeout is configured                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |



| Recommendation |                                                                                                                                                          | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                          | Yes                      | No                       |
| 5.4.3.3        | Ensure default user umask is configured                                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.5        | Ensure the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.6        | Ensure the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.8        | Ensure the umask default for installed shells is "077"                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.9        | Ensure the default umask for all local interactive users is "077"                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.10       | Ensure the operating system initiates a session lock after 15 minutes of inactivity                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.11       | Ensure the operating system prevents users from disabling the tmux terminal multiplexer                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.12       | Ensure the operating system's shell initialization file is configured to start each shell with the tmux terminal multiplexer                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.13       | Ensure the operating system enables the user to initiate a session lock                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.16       | Ensure StopIdleSessionSec is configured                                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.1      | Ensure journald service is enabled and active                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.2      | Ensure journald log file access is configured                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.3      | Ensure journald log file rotation is configured                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.5      | Ensure journald Storage is configured                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.6      | Ensure journald Compress is configured                                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.1      | Ensure systemd-journal-remote is installed                                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.2      | Ensure systemd-journal-remote authentication is configured                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.3      | Ensure systemd-journal-upload is enabled and active                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.1        | Ensure rsyslog is installed                                                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.2        | Ensure rsyslog service is enabled and active                                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.4        | Ensure journald is configured to send logs to rsyslog                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.5        | Ensure rsyslog log file creation mode is configured                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.6        | Ensure rsyslog logging is configured                                                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                  | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                  | Yes                      | No                       |
| 6.2.2.7        | Ensure rsyslog is configured to send logs to a remote log host                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.11       | Ensure the rsyslog service is enabled and active                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.1        | Ensure access to all logfiles has been configured                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.2        | Ensure /var/log/messages mode is configured                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.3        | Ensure /var/log/messages owner is configured                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.4        | Ensure /var/log/messages group owner is configured                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.5        | Ensure /var/log is mode is configured                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.6        | Ensure /var/log owner is configured                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.7        | Ensure /var/log group owner is configured                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.8        | Ensure administrators are notified if an audit processing failure occurs by modifying /etc/aliases                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.1        | Ensure auditd packages are installed                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.2        | Ensure auditing for processes that start prior to auditd is enabled                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.3        | Ensure audit_backlog_limit is sufficient                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.4        | Ensure auditd service is enabled and active                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.5        | Ensure the operating system allocates a sufficient audit_backlog_limit to capture processes that start prior to the audit daemon | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.6        | Ensure the operating system's audit daemon is configured to include local events                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.8        | Ensure the operating system's audit daemon is configured to resolve audit information before writing to disk                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.6        | Ensure the SA and ISSO are notified in the event of an audit processing failure                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.6        | Ensure use of privileged commands are collected                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.12       | Ensure login and logout events are collected                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.13       | Ensure file deletion events by users are collected                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.15       | Ensure successful and unsuccessful attempts to use the chcon command are collected                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.16       | Ensure successful and unsuccessful attempts to use the setfacl command are collected                                             | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                  | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                  | Yes                      | No                       |
| 6.3.3.17       | Ensure successful and unsuccessful attempts to use the chacl command are collected               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.18       | Ensure successful and unsuccessful attempts to use the usermod command are collected             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.19       | Ensure kernel module loading unloading and modification is collected                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.20       | Ensure the audit configuration is immutable                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.24       | Ensure successful and unsuccessful attempts to use the chsh command are collected                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.25       | Ensure successful and unsuccessful attempts to use the crontab command are collected             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.26       | Ensure successful and unsuccessful attempts to use the gpasswd command are collected             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.27       | Ensure successful and unsuccessful attempts to use the newgrp command are collected              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.28       | Ensure successful and unsuccessful attempts to use the pam_timestamp_check command are collected | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.29       | Ensure successful and unsuccessful attempts to use the ssh-keysign command are collected         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.30       | Ensure successful and unsuccessful attempts to use the unix_chkpwd command are collected         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.31       | Ensure successful and unsuccessful attempts to use the setsebool command are collected           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.32       | Ensure successful and unsuccessful attempts to use the userhelper command are collected          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.33       | Ensure successful and unsuccessful attempts to use the setfiles command are collected            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.34       | Ensure successful and unsuccessful attempts to use the semanage command are collected            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.35       | Ensure successful and unsuccessful attempts to use the postqueue command are collected           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.36       | Ensure successful and unsuccessful attempts to use the postdrop command are collected            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.37       | Ensure successful and unsuccessful attempts to use the unix_update command are collected         | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                        | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                        | Yes                      | No                       |
| 6.3.3.38       | Ensure successful and unsuccessful attempts to use the umount command are collected    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.39       | Ensure successful and unsuccessful attempts to use the mount command are collected     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.40       | Ensure successful and unsuccessful attempts to use the ssh-agent command are collected | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.41       | Ensure successful and unsuccessful attempts to use the passwd command are collected    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.42       | Ensure successful and unsuccessful attempts to use the chage command are collected     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.43       | Ensure the audit system prevents unauthorized changes to logon UIDs                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.44       | Ensure successful and unsuccessful modifications to the faillock file are collected    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.1        | Ensure the audit log file directory mode is configured                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.2        | Ensure audit log files mode is configured                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.3        | Ensure audit log files owner is configured                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.4        | Ensure audit log files group owner is configured                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.5        | Ensure audit configuration files mode is configured                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.6        | Ensure audit configuration files owner is configured                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.7        | Ensure audit configuration files group owner is configured                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.8        | Ensure audit tools mode is configured                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.9        | Ensure audit tools owner is configured                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.10       | Ensure audit tools group owner is configured                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.11       | Ensure the audit logs are group-owned by root                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.12       | Ensure audit tools are mode 0755 or more restrictive                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.13       | Ensure the audit tools are owned by root                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.14       | Ensure audit tools are group owned by root                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.15       | Ensure the audit log file directories are mode 0700 or more restrictive                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.16       | Ensure the audit log file directory is owned by root                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.17       | Ensure audit log files group owner is root                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.18       | Ensure audit log files are mode 0600 or more restrictive                               | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                           | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                           | Yes                      | No                       |
| 7.1.1          | Ensure permissions on /etc/passwd are configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.2          | Ensure permissions on /etc/passwd- are configured                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.3          | Ensure permissions on /etc/group are configured                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.4          | Ensure permissions on /etc/group- are configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.5          | Ensure permissions on /etc/shadow are configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.6          | Ensure permissions on /etc/shadow- are configured                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.9          | Ensure permissions on /etc/shells are configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.10         | Ensure permissions on /etc/security/opasswd are configured                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.11         | Ensure world writable files and directories are secured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.12         | Ensure no files or directories without an owner and a group exist                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.13         | Ensure SUID and SGID files are reviewed                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.16         | Ensure system-wide shared library directories have mode 755 or less permissive                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.17         | Ensure system-wide shared library directories must be owned by root                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.18         | Ensure the system-wide shared library directories are group-owned by root or a system account                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.19         | Ensure world-writable directories owner is configured                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.20         | Ensure world-writable directories group-owner is configured                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.21         | Ensure local initialization files do not execute world-writable programs                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.22         | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are mode 0755 or more restrictive | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.23         | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are owned by root                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.24         | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are group-owned by root           | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.25         | Ensure the system-wide shared library files are mode 0755 or more restrictive                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.26         | Ensure the system-wide shared library files are owned by root                                                             | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                       | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                       | Yes                      | No                       |
| 7.1.27         | Ensure the system-wide shared library files are group-owned by root                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.4          | Ensure shadow group is empty                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.9          | Ensure local interactive user home directories are configured                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.10         | Ensure local interactive user dot files access is configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.11         | Ensure all files and directories in the local interactive user home directory are group-owned by a group that the user is a member of | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.12         | Ensure all files and directories in a local interactive user home directory are mode 0750 or more restrictive                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.13         | Ensure all local initialization files are mode 0740 or more restrictive                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.14         | Ensure local interactive user home directories group-owner is their primary GID                                                       | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: CIS Controls v7 IG 2 Mapped Recommendations

| Recommendation |                                                                                           | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                           | Yes                      | No                       |
| 1.1.1.1        | Ensure cramfs kernel module is not available                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.2        | Ensure freevxfs kernel module is not available                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.3        | Ensure hfs kernel module is not available                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.4        | Ensure hfsplus kernel module is not available                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.5        | Ensure jffs2 kernel module is not available                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.6        | Ensure overlayfs kernel module is not available                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.7        | Ensure squashfs kernel module is not available                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.8        | Ensure udf kernel module is not available                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.9        | Ensure usb-storage kernel module is not available                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.10       | Ensure unused filesystems kernel modules are not available                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.11       | Ensure the operating system disables the ability to load the firewire-core kernel module  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.12       | Ensure a camera is not installed                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.1      | Ensure /tmp is a separate partition                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.2      | Ensure nodev option set on /tmp partition                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.3      | Ensure nosuid option set on /tmp partition                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.4      | Ensure noexec option set on /tmp partition                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.1      | Ensure /dev/shm is a separate partition                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.2      | Ensure nodev option set on /dev/shm partition                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.3      | Ensure nosuid option set on /dev/shm partition                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.4      | Ensure noexec option set on /dev/shm partition                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.1      | Ensure separate partition exists for /home                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.2      | Ensure nodev option set on /home partition                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.3      | Ensure nosuid option set on /home partition                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.5      | Ensure file systems that contain user home directories are mounted with the nosuid option | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                             | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                             | Yes                      | No                       |
| 1.1.2.3.6      | Ensure file systems that contain user home directories are mounted with the "noexec" option | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.4.1      | Ensure separate partition exists for /var                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.4.2      | Ensure nodev option set on /var partition                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.4.3      | Ensure nosuid option set on /var partition                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.1      | Ensure separate partition exists for /var/tmp                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.2      | Ensure nodev option set on /var/tmp partition                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.3      | Ensure nosuid option set on /var/tmp partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.4      | Ensure noexec option set on /var/tmp partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.1      | Ensure separate partition exists for /var/log                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.2      | Ensure nodev option set on /var/log partition                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.3      | Ensure nosuid option set on /var/log partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.4      | Ensure noexec option set on /var/log partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.1      | Ensure separate partition exists for /var/log/audit                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.2      | Ensure nodev option set on /var/log/audit partition                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.3      | Ensure nosuid option set on /var/log/audit partition                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.4      | Ensure noexec option set on /var/log/audit partition                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.8.1      | Ensure the "/boot" directory is mounted with the "nosuid" option                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.9.1      | Ensure the "/boot/efi" directory is mounted with the "nosuid" option                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.10.1     | Ensure file systems that are being NFS-imported are mounted with the "nodev" option         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.10.2     | Ensure file systems being imported via NFS are mounted with the "nosuid" option             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.10.3     | Ensure file systems being imported via NFS are mounted with the "noexec" option             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.11.1     | Ensure nodev option set on removable media partitions                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.11.2     | Ensure nosuid option set on removable media partitions                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.11.3     | Ensure noexec option set on removable media partitions                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.12       | Ensure all non-root local partitions are mounted with the "nodev" option                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.1        | Ensure GPG keys are configured                                                              | <input type="checkbox"/> | <input type="checkbox"/> |



| Recommendation |                                                                                      | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                      | Yes                      | No                       |
| 1.2.1.2        | Ensure gpgcheck is globally activated                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.3        | Ensure repo_gpgcheck is globally activated                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.4        | Ensure package manager repositories are configured                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.5        | Ensure DNF is configured to perform a signature check on local packages              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2.1        | Ensure updates, patches, and additional security software are installed              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2.2        | Ensure vendor packaged system security patches and updates are installed             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.1        | Ensure SELinux is installed                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.2        | Ensure SELinux is not disabled in bootloader configuration                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.3        | Ensure SELinux policy is configured                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.4        | Ensure the SELinux mode is not disabled                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.5        | Ensure the SELinux mode is enforcing                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.6        | Ensure no unconfined services exist                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.7        | Ensure the MCS Translation Service (mcstrans) is not installed                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.8        | Ensure the operating system has the polycoreutils package installed                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.9        | Ensure SETroubleshoot is not installed                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.10       | Ensure SELinux prevents nonprivileged users from executing privileged functions      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.1          | Ensure bootloader password is set                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.2          | Ensure access to bootloader config is configured                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.3          | Ensure the operating system requires authentication for rescue mode                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.4          | Ensure the operating system requires authentication upon booting into emergency mode | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.5          | Ensure a unique name is set as the superusers account (BIOS)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.6          | Ensure a unique name is set as the superusers account (UEFI)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1          | Ensure address space layout randomization is enabled                                 | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                     | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                     | Yes                      | No                       |
| 1.5.2          | Ensure ptrace_scope is restricted                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.8          | Ensure the operating system enables hardening for the BPF JIT                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.10         | Ensure the NX (no-execution) bit flag is set on the system                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.11         | Ensure the operating system disables the use of user namespaces                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.13         | Ensure the operating system is configured to enable DAC on symlinks                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.15         | Ensure the operating system is configured to enable DAC on hardlinks                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.16         | Ensure the operating system restricts exposed kernel pointer addresses access                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.17         | Ensure the operating system is configured to restrict access to the kernel message buffer                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.19         | Ensure the operating system is configured to prevent kernel profiling by unprivileged users                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.20         | Ensure the operating system restricts usage of ptrace to descendant processes                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.21         | Ensure the operating system prevents privilege escalation through the kernel by disabling access to the bpf syscall | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.23         | Ensure the operating system implements the Endpoint Security for Linux Threat Prevention tool                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.1          | Ensure system wide crypto policy is not set to legacy                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.2          | Ensure system wide crypto policy is not set in sshd configuration                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.3          | Ensure system wide crypto policy disables sha1 hash and signature support                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.4          | Ensure system wide crypto policy disables macs less than 128 bits                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.5          | Ensure system wide crypto policy disables cbc for ssh                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.6          | Ensure system wide crypto policy disables chacha20-poly1305 for ssh                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.7          | Ensure system wide crypto policy disables EtM for ssh                                                               | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                  | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                  | Yes                      | No                       |
| 1.6.8          | Ensure system-wide crypto policy is FIPS                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.10         | Ensure system-wide crypto policies are in effect                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.12         | Ensure the OpenSSL library is configured to use only ciphers employing FIPS 140-2-approved algorithms                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.13         | Ensure the OpenSSL library is configured to use only DoD-approved TLS encryption                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.14         | Ensure the GnuTLS library is configured to only allow DoD-approved SSL/TLS Versions                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.4          | Ensure access to /etc/motd is configured                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.5          | Ensure access to /etc/issue is configured                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.6          | Ensure access to /etc/issue.net is configured                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.1          | Ensure GNOME Display Manager is removed                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.4          | Ensure GDM screen locks when the user is idle                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.5          | Ensure GDM screen locks cannot be overridden                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.6          | Ensure GDM automatic mounting of removable media is disabled                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.7          | Ensure GDM disabling automatic mounting of removable media is not overridden                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.8          | Ensure the operating system does not allow an unattended or automatic logon to the system via a graphical user interface         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.9          | Ensure GDM autorun-never is enabled                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.11         | Ensure GDM autorun-never is not overridden                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.12         | Ensure the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.13         | Ensure XDMCP is not enabled                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.14         | Ensure the operating system disables the user logon list for graphical user interfaces                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.16         | Ensure the operating system prevents users from overriding the session idle-delay setting for the graphical user interface       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.17         | Ensure the operating system prevents users from overriding the screensaver lock-enabled setting for the graphical user interface | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                 | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                 | Yes                      | No                       |
| 1.8.19         | Ensure the operating system enables a user's session lock until that user re-establishes access | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.9            | Ensure the "tmux" package installed                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.13           | Ensure the operating system has the packages required for multifactor authentication            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.1          | Ensure autofs services are not in use                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.2          | Ensure avahi daemon services are not in use                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.3          | Ensure dhcp server services are not in use                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4          | Ensure dns server services are not in use                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.5          | Ensure dnsmasq services are not in use                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.6          | Ensure ftp server services are not in use                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.7          | Ensure message access server services are not in use                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.8          | Ensure network file system services are not in use                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.9          | Ensure nis server services are not in use                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.10         | Ensure print server services are not in use                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.11         | Ensure rpcbind services are not in use                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.12         | Ensure rsync services are not in use                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.13         | Ensure samba file server services are not in use                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.14         | Ensure snmp services are not in use                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.15         | Ensure telnet server services are not in use                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.16         | Ensure tftp server services are not in use                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.17         | Ensure web proxy server services are not in use                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.18         | Ensure web server services are not in use                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.19         | Ensure xinetd services are not in use                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.20         | Ensure X window server services are not in use                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.21         | Ensure only approved services are listening on a network interface                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.22         | Ensure automated bug reporting tools are not installed                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.23         | Ensure mail transfer agents are configured for local-only mode                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.24         | Ensure the sendmail package is not installed                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.25         | Ensure the rsh-server package is not installed                                                  | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                 | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                 | Yes                      | No                       |
| 2.1.26         | Ensure system daemons are prevented from using Kerberos for authentication                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.27         | Ensure the operating system is configured to mask the debug-shell systemd service                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.28         | Ensure the gssproxy package has not been installed on the system                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.29         | Ensure the iprutils package has not been installed on the system                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.30         | Ensure the krb5-server package has not been installed on the system                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.31         | Ensure a TFTP server has not been installed on the system                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.32         | Ensure the tuned package has not been installed on the system                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.34         | Ensure the operating system is configured to prevent unrestricted mail relaying                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.1          | Ensure ftp client is not installed                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.2          | Ensure ldap client is not installed                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.3          | Ensure nis client is not installed                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.4          | Ensure telnet client is not installed                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.5          | Ensure tftp client is not installed                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.6          | Ensure krb5-workstation is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.1          | Ensure time synchronization is in use                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.2          | Ensure chrony is configured                                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.4          | Ensure the operating system is securely comparing internal information system clocks at least every 24 hours with an NTP server | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.5          | Ensure the operating system disables network management of the chrony daemon                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.6          | Ensure the operating system disables the chrony daemon from acting as a server                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.2        | Ensure permissions on /etc/crontab are configured                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.3        | Ensure permissions on /etc/cron.hourly are configured                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.4        | Ensure permissions on /etc/cron.daily are configured                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                | Yes                      | No                       |
| 2.4.1.5        | Ensure permissions on /etc/cron.weekly are configured                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.6        | Ensure permissions on /etc/cron.monthly are configured                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.7        | Ensure permissions on /etc/cron.d are configured                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.8        | Ensure crontab is restricted to authorized users                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.2.1        | Ensure at is restricted to authorized users                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5.1          | Ensure USBGuard is installed on the operating system                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5.2          | Ensure USBGuard has a policy configured                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5.3          | Ensure the operating system enables Linux audit logging of the USBGuard daemon | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5.4          | Ensure the usbguard service is enabled and active                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.6.2          | Ensure fapolicyd employs a deny-all, permit-by-exception policy                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.6.3          | Ensure fapolicyd is enabled and running                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1.1          | Ensure IPv6 status is identified                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1.3          | Ensure bluetooth services are not in use                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1.4          | Ensure network interfaces are not in promiscuous mode                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.1          | Ensure dccp kernel module is not available                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.2          | Ensure tipc kernel module is not available                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.3          | Ensure rds kernel module is not available                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.4          | Ensure sctp kernel module is not available                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.5          | Ensure atm kernel module is not available                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.6          | Ensure bluetooth kernel module is not available                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.7          | Ensure can kernel module is not available                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.1          | Ensure ip forwarding is disabled                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.2          | Ensure packet redirect sending is disabled                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.3          | Ensure bogus icmp responses are ignored                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.4          | Ensure broadcast icmp requests are ignored                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.5          | Ensure icmp redirects are not accepted                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.6          | Ensure secure icmp redirects are not accepted                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.7          | Ensure reverse path filtering is enabled                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.8          | Ensure source routed packets are not accepted                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.9          | Ensure suspicious packets are logged                                           | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                            | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                            | Yes                      | No                       |
| 3.3.10         | Ensure tcp syn cookies is enabled                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.11         | Ensure ipv6 router advertisements are not accepted                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.12         | Ensure net.ipv4.conf.all.forwarding is disabled                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.1        | Ensure nftables base chains exist                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.2        | Ensure host based firewall loopback traffic is configured                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.3        | Ensure firewalld drops unnecessary services and ports                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.4        | Ensure nftables established connections are configured                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.5        | Ensure nftables default deny firewall policy                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2          | Ensure the firewall is configured to remove unnecessary use of functions, ports, protocols, and/or services                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.3          | Ensure firewalld service is enabled and running                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.4          | Ensure nftables is installed                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.5          | Ensure a single firewall configuration utility is in use                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.6          | Ensure "nftables" is configured to allow rate limits on any connection to the system                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.7          | Ensure "firewalld" is installed                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.8          | Ensure "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1          | Ensure openssh-server is installed                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2          | Ensure permissions on /etc/ssh/sshd_config are configured                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3          | Ensure permissions on SSH private host key files are configured                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.4          | Ensure permissions on SSH public host key files are configured                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.5          | Ensure sshd access is configured                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.7          | Ensure sshd Ciphers are configured                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.9          | Ensure sshd DisableForwarding is enabled                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.10         | Ensure sshd GSSAPIAuthentication is disabled                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.12         | Ensure sshd IgnoreRhosts is enabled                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.13         | Ensure sshd KexAlgorithms is configured                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.15         | Ensure sshd LogLevel is configured                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                               | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                               | Yes                      | No                       |
| 5.1.16         | Ensure sshd MACs are configured                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.20         | Ensure sshd PermitEmptyPasswords is disabled                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.21         | Ensure sshd PermitRootLogin is disabled                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.23         | Ensure sshd UsePAM is enabled                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.24         | Ensure sshd private key files have a passcode                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.25         | Ensure sshd X11Forwarding is disabled                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.26         | Ensure sshd ClientAliveInterval is configured                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.27         | Ensure sshd ClientAliveCountMax is configured                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.28         | Ensure the SSH server is configured to use only MACs employing FIPS 140-2-approved algorithms                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.29         | Ensure the SSH server is configured to use only ciphers employing FIPS 140-2-approved algorithms              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.30         | Ensure sshd is configured to use only FIPS-validated key exchange algorithms                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.31         | Ensure the SSH server uses strong entropy                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.34         | Ensure sshd IgnoreUserKnownHosts is enabled                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.36         | Ensure sshd KerberosAuthentication is disabled                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.37         | Ensure sshd RekeyLimit is configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.39         | Ensure SSH is loaded and active                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1          | Ensure sudo is installed                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3          | Ensure sudo commands use pty                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4          | Ensure sudo log file exists                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.5          | Ensure users must provide password for escalation                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.6          | Ensure the sudoers file restricts sudo access to authorized personnel                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.7          | Ensure re-authentication for privilege escalation is not disabled globally                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.8          | Ensure the sudoers security policy is configured to use the invoking user's password for privilege escalation | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.9          | Ensure sudo timestamp_timeout is configured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.10         | Ensure access to the su command is restricted                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.11         | Ensure pam_succeed_if does not exist in /etc/pam.d/sudo                                                       | <input type="checkbox"/> | <input type="checkbox"/> |



| Recommendation |                                                                                                                              | Set Correctly            |                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                              | Yes                      | No                       |
| 5.3.2.1        | Ensure active authselect profile includes pam modules                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.2        | Ensure pam_faillock module is enabled                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.3        | Ensure pam_pwquality module is enabled                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.4        | Ensure pam_pwhistory module is enabled                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.1      | Ensure password failed attempts lockout is configured                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.2      | Ensure password unlock time is configured                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.3      | Ensure password failed attempts lockout includes root account                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.4      | Ensure deny is configured on the pam_faillock module                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.5      | Ensure deny is configured in /etc/security/faillock.conf                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.6      | Ensure fail_interval is configured on the pam_faillock module                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.7      | Ensure fail_interval is configured in /etc/security/faillock.conf                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.8      | Ensure unlock_time is configured on the pam_faillock module                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.9      | Ensure unlock_time is configured in /etc/security/faillock.conf                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.10     | Ensure dir is configured on the pam_faillock module                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.11     | Ensure dir is configured in /etc/security/faillock.conf                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.14     | Ensure audit is set on the pam_faillock module                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.15     | Ensure audit is set in /etc/security/faillock.conf                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.16     | Ensure even_deny_root is set on the pam_faillock module                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.17     | Ensure even_deny_root is set in /etc/security/faillock.conf                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.18     | Ensure the use of a non-default faillock tally directory while SELinux enforces a targeted policy                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.19     | Ensure the use of a non-default faillock tally directory on the pam_faillock module while SELinux enforces a targeted policy | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.1      | Ensure password number of changed characters is configured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.2      | Ensure password length is configured                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.3      | Ensure password complexity is configured                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                     | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                     | Yes                      | No                       |
| 5.3.3.2.4      | Ensure password same consecutive characters is configured                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.5      | Ensure password maximum sequential characters is configured                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.6      | Ensure password dictionary check is enabled                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.7      | Ensure password quality is enforced for the root user                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.8      | Ensure the operating system enforces a minimum 15-character password length         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.9      | Ensure ucredit is configured in /etc/security/pwquality.conf                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.10     | Ensure lcredit is configured in /etc/security/pwquality.conf                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.11     | Ensure dcredit is configured in /etc/security/pwquality.conf                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.12     | Ensure ocredit is configured in /etc/security/pwquality.conf                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.13     | Ensure maxclassrepeat is configured in /etc/security/pwquality.conf                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.14     | Ensure minclass is configured in /etc/security/pwquality.conf                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.15     | Ensure difok is configured in /etc/security/pwquality.conf                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.16     | Ensure dictcheck is configured                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.17     | Ensure retry is configured on the pam_pwquality module in /etc/pam.d/system-auth    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.18     | Ensure retry is configured on the pam_pwquality module in /etc/pam.d/password-auth  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.19     | Ensure retry is configured in /etc/security/pwquality.conf                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.1      | Ensure password history remember is configured                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.2      | Ensure password history is enforced for the root user                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.3      | Ensure pam_pwhistory includes use_authtok                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.5      | Ensure remember is configured on the pam_pwhistory module in /etc/pam.d/system-auth | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.1      | Ensure pam_unix does not include nullok                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.2      | Ensure pam_unix does not include remember                                           | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                   | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                   | Yes                      | No                       |
| 5.3.3.4.3      | Ensure pam_unix includes a strong password hashing algorithm                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.4      | Ensure pam_unix includes use_authok                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.5      | Ensure pam_unix includes a FIPS 140-2 approved hashing algorithm                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.6.1      | Ensure the operating system uses multifactor authentication for local access to accounts                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.6.3      | Ensure the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.1        | Ensure password expiration is configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.2        | Ensure minimum password days is configured                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.3        | Ensure password expiration warning days is configured                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.4        | Ensure strong password hashing algorithm is configured                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.5        | Ensure inactive password lock is configured                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.6        | Ensure all users last password change date is in the past                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.7        | Ensure passwords use FIPS 140-2 approved cryptographic hashing algorithm                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.8        | Ensure minimum number of hashing rounds is configured                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.9        | Ensure existing passwords use FIPS 140-2 approved cryptographic hashing algorithm                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.12       | Ensure pass_min_len is configured                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.13       | Ensure the maximum time period for existing passwords is restricted to 60 days                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.2        | Ensure root is the only GID 0 account                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.3        | Ensure group root is the only GID 0 group                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.4        | Ensure root account access is controlled                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.6        | Ensure root user umask is configured                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.7        | Ensure system accounts do not have a valid login shell                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.8        | Ensure accounts without a valid login shell are locked                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.2        | Ensure default user shell timeout is configured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.3        | Ensure default user umask is configured                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.5        | Ensure the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                                          | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                          | Yes                      | No                       |
| 5.4.3.6        | Ensure the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.7        | Ensure the operating system enforces a 60-day maximum password lifetime for new user accounts                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.8        | Ensure the umask default for installed shells is "077"                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.9        | Ensure the default umask for all local interactive users is "077"                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.10       | Ensure the operating system initiates a session lock after 15 minutes of inactivity                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.11       | Ensure the operating system prevents users from disabling the tmux terminal multiplexer                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.12       | Ensure the operating system's shell initialization file is configured to start each shell with the tmux terminal multiplexer                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.13       | Ensure the operating system enables the user to initiate a session lock                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.16       | Ensure StopIdleSessionSec is configured                                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.1      | Ensure journald service is enabled and active                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.2      | Ensure journald log file access is configured                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.3      | Ensure journald log file rotation is configured                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.4      | Ensure journald ForwardToSyslog is disabled                                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.5      | Ensure journald Storage is configured                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.6      | Ensure journald Compress is configured                                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.1      | Ensure systemd-journal-remote is installed                                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.2      | Ensure systemd-journal-remote authentication is configured                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.3      | Ensure systemd-journal-upload is enabled and active                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.4      | Ensure systemd-journal-remote service is not in use                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.1        | Ensure rsyslog is installed                                                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.2        | Ensure rsyslog service is enabled and active                                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.3        | Ensure all remote access methods are monitored                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.4        | Ensure journald is configured to send logs to rsyslog                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.5        | Ensure rsyslog log file creation mode is configured                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                  | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                  | Yes                      | No                       |
| 6.2.2.6        | Ensure rsyslog logging is configured                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.7        | Ensure rsyslog is configured to send logs to a remote log host                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.8        | Ensure rsyslog is not configured to receive logs from a remote client                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.9        | Ensure logrotate is configured                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.10       | Ensure rsyslog is configured to log cron events                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.11       | Ensure the rsyslog service is enabled and active                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.12       | Ensure the operating system has the packages required for encrypting offloaded audit logs                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.13       | Ensure the the operating system authenticates the remote logging server for off-loading audit logs                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.14       | Ensure the operating system encrypts audit records off-loaded onto a different system or media from the system being audited     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.15       | Ensure the audit system off-loads audit records onto a different system or media from the system being audited                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.1        | Ensure access to all logfiles has been configured                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.2        | Ensure /var/log/messages mode is configured                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.3        | Ensure /var/log/messages owner is configured                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.4        | Ensure /var/log/messages group owner is configured                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.5        | Ensure /var/log is mode is configured                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.6        | Ensure /var/log owner is configured                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.7        | Ensure /var/log group owner is configured                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.8        | Ensure administrators are notified if an audit processing failure occurs by modifying /etc/aliases                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.1        | Ensure auditd packages are installed                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.2        | Ensure auditing for processes that start prior to auditd is enabled                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.3        | Ensure audit_backlog_limit is sufficient                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.4        | Ensure auditd service is enabled and active                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.5        | Ensure the operating system allocates a sufficient audit_backlog_limit to capture processes that start prior to the audit daemon | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                                                | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                                | Yes                      | No                       |
| 6.3.1.6        | Ensure the operating system's audit daemon is configured to include local events                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.7        | Ensure the operating system's audit daemon is configured to label all off-loaded audit logs                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.8        | Ensure the operating system's audit daemon is configured to resolve audit information before writing to disk                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.1        | Ensure audit log storage size is configured                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.2        | Ensure audit logs are not automatically deleted                                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.5        | Ensure the operating system allocates audit record storage capacity                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.6        | Ensure the SA and ISSO are notified in the event of an audit processing failure                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.7        | Ensure the operating system notifies the SA and ISSO when allocated audit record storage volume reaches 75 percent                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.8        | Ensure the operating system takes action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.9        | Ensure the audit system is configured to take an appropriate action when the internal event queue is full                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.1        | Ensure changes to system administration scope (sudoers) is collected                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.2        | Ensure actions as another user are always logged                                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.3        | Ensure events that modify the sudo log file are collected                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.4        | Ensure events that modify date and time information are collected                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.5        | Ensure events that modify the system's network environment are collected                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.6        | Ensure use of privileged commands are collected                                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.8        | Ensure events that modify user/group information are collected                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.9        | Ensure discretionary access control permission modification events are collected                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.10       | Ensure successful file system mounts are collected                                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                  | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                  | Yes                      | No                       |
| 6.3.3.11       | Ensure session initiation information is collected                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.12       | Ensure login and logout events are collected                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.13       | Ensure file deletion events by users are collected                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.14       | Ensure events that modify the system's Mandatory Access Controls are collected                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.15       | Ensure successful and unsuccessful attempts to use the chcon command are collected               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.16       | Ensure successful and unsuccessful attempts to use the setfacl command are collected             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.17       | Ensure successful and unsuccessful attempts to use the chacl command are collected               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.18       | Ensure successful and unsuccessful attempts to use the usermod command are collected             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.19       | Ensure kernel module loading unloading and modification is collected                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.20       | Ensure the audit configuration is immutable                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.21       | Ensure the running and on disk configuration is the same                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.22       | Ensure successful and unsuccessful attempts to use the su command are collected                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.23       | Ensure successful and unsuccessful attempts to use the sudo command are collected                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.24       | Ensure successful and unsuccessful attempts to use the chsh command are collected                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.25       | Ensure successful and unsuccessful attempts to use the crontab command are collected             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.26       | Ensure successful and unsuccessful attempts to use the gpasswd command are collected             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.27       | Ensure successful and unsuccessful attempts to use the newgrp command are collected              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.28       | Ensure successful and unsuccessful attempts to use the pam_timestamp_check command are collected | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.29       | Ensure successful and unsuccessful attempts to use the ssh-keysign command are collected         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.30       | Ensure successful and unsuccessful attempts to use the unix_chkpwd command are collected         | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                          | Set Correctly            |                          |
|----------------|------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                          | Yes                      | No                       |
| 6.3.3.31       | Ensure successful and unsuccessful attempts to use the setsebool command are collected   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.32       | Ensure successful and unsuccessful attempts to use the userhelper command are collected  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.33       | Ensure successful and unsuccessful attempts to use the setfiles command are collected    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.34       | Ensure successful and unsuccessful attempts to use the semanage command are collected    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.35       | Ensure successful and unsuccessful attempts to use the postqueue command are collected   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.36       | Ensure successful and unsuccessful attempts to use the postdrop command are collected    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.37       | Ensure successful and unsuccessful attempts to use the unix_update command are collected | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.38       | Ensure successful and unsuccessful attempts to use the umount command are collected      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.39       | Ensure successful and unsuccessful attempts to use the mount command are collected       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.40       | Ensure successful and unsuccessful attempts to use the ssh-agent command are collected   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.41       | Ensure successful and unsuccessful attempts to use the passwd command are collected      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.42       | Ensure successful and unsuccessful attempts to use the chage command are collected       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.43       | Ensure the audit system prevents unauthorized changes to logon UIDs                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.44       | Ensure successful and unsuccessful modifications to the faillock file are collected      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.1        | Ensure the audit log file directory mode is configured                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.2        | Ensure audit log files mode is configured                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.3        | Ensure audit log files owner is configured                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.4        | Ensure audit log files group owner is configured                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.5        | Ensure audit configuration files mode is configured                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.6        | Ensure audit configuration files owner is configured                                     | <input type="checkbox"/> | <input type="checkbox"/> |



| Recommendation |                                                                         | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                         | Yes                      | No                       |
| 6.3.4.7        | Ensure audit configuration files group owner is configured              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.8        | Ensure audit tools mode is configured                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.9        | Ensure audit tools owner is configured                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.10       | Ensure audit tools group owner is configured                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.11       | Ensure the audit logs are group-owned by root                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.12       | Ensure audit tools are mode 0755 or more restrictive                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.13       | Ensure the audit tools are owned by root                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.14       | Ensure audit tools are group owned by root                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.15       | Ensure the audit log file directories are mode 0700 or more restrictive | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.16       | Ensure the audit log file directory is owned by root                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.17       | Ensure audit log files group owner is root                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.18       | Ensure audit log files are mode 0600 or more restrictive                | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.1          | Ensure permissions on /etc/passwd are configured                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.2          | Ensure permissions on /etc/passwd- are configured                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.3          | Ensure permissions on /etc/group are configured                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.4          | Ensure permissions on /etc/group- are configured                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.5          | Ensure permissions on /etc/shadow are configured                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.6          | Ensure permissions on /etc/shadow- are configured                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.7          | Ensure permissions on /etc/gshadow are configured                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.8          | Ensure permissions on /etc/gshadow- are configured                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.9          | Ensure permissions on /etc/shells are configured                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.10         | Ensure permissions on /etc/security/opasswd are configured              | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.11         | Ensure world writable files and directories are secured                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.12         | Ensure no files or directories without an owner and a group exist       | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.13         | Ensure SUID and SGID files are reviewed                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.14         | Ensure there are no ".shosts" files on the operating system             | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.15         | Ensure there are no "shosts.equiv" files on the operating system        | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                       | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                       | Yes                      | No                       |
| 7.1.16         | Ensure system-wide shared library directories have mode 755 or less permissive                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.17         | Ensure system-wide shared library directories must be owned by root                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.18         | Ensure the system-wide shared library directories are group-owned by root or a system account                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.19         | Ensure world-writable directories owner is configured                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.20         | Ensure world-writable directories group-owner is configured                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.21         | Ensure local initialization files do not execute world-writable programs                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.22         | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are mode 0755 or more restrictive             | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.23         | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are owned by root                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.24         | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are group-owned by root                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.25         | Ensure the system-wide shared library files are mode 0755 or more restrictive                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.26         | Ensure the system-wide shared library files are owned by root                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.27         | Ensure the system-wide shared library files are group-owned by root                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.1          | Ensure accounts in /etc/passwd use shadowed passwords                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.2          | Ensure /etc/shadow password fields are not empty                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.4          | Ensure shadow group is empty                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.9          | Ensure local interactive user home directories are configured                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.10         | Ensure local interactive user dot files access is configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.11         | Ensure all files and directories in the local interactive user home directory are group-owned by a group that the user is a member of | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                               | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                               | Yes                      | No                       |
| 7.2.12         | Ensure all files and directories in a local interactive user home directory are mode 0750 or more restrictive | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.13         | Ensure all local initialization files are mode 0740 or more restrictive                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.14         | Ensure local interactive user home directories group-owner is their primary GID                               | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: CIS Controls v7 IG 3 Mapped Recommendations

| Recommendation |                                                                                           | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                           | Yes                      | No                       |
| 1.1.1.1        | Ensure cramfs kernel module is not available                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.2        | Ensure freevxfs kernel module is not available                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.3        | Ensure hfs kernel module is not available                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.4        | Ensure hfsplus kernel module is not available                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.5        | Ensure jffs2 kernel module is not available                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.6        | Ensure overlayfs kernel module is not available                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.7        | Ensure squashfs kernel module is not available                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.8        | Ensure udf kernel module is not available                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.9        | Ensure usb-storage kernel module is not available                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.10       | Ensure unused filesystems kernel modules are not available                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.11       | Ensure the operating system disables the ability to load the firewire-core kernel module  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.12       | Ensure a camera is not installed                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.1      | Ensure /tmp is a separate partition                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.2      | Ensure nodev option set on /tmp partition                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.3      | Ensure nosuid option set on /tmp partition                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.4      | Ensure noexec option set on /tmp partition                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.1      | Ensure /dev/shm is a separate partition                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.2      | Ensure nodev option set on /dev/shm partition                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.3      | Ensure nosuid option set on /dev/shm partition                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.4      | Ensure noexec option set on /dev/shm partition                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.1      | Ensure separate partition exists for /home                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.2      | Ensure nodev option set on /home partition                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.3      | Ensure nosuid option set on /home partition                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.5      | Ensure file systems that contain user home directories are mounted with the nosuid option | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                             | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                             | Yes                      | No                       |
| 1.1.2.3.6      | Ensure file systems that contain user home directories are mounted with the "noexec" option | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.4.1      | Ensure separate partition exists for /var                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.4.2      | Ensure nodev option set on /var partition                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.4.3      | Ensure nosuid option set on /var partition                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.1      | Ensure separate partition exists for /var/tmp                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.2      | Ensure nodev option set on /var/tmp partition                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.3      | Ensure nosuid option set on /var/tmp partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.4      | Ensure noexec option set on /var/tmp partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.1      | Ensure separate partition exists for /var/log                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.2      | Ensure nodev option set on /var/log partition                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.3      | Ensure nosuid option set on /var/log partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.4      | Ensure noexec option set on /var/log partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.1      | Ensure separate partition exists for /var/log/audit                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.2      | Ensure nodev option set on /var/log/audit partition                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.3      | Ensure nosuid option set on /var/log/audit partition                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.4      | Ensure noexec option set on /var/log/audit partition                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.8.1      | Ensure the "/boot" directory is mounted with the "nosuid" option                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.9.1      | Ensure the "/boot/efi" directory is mounted with the "nosuid" option                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.10.1     | Ensure file systems that are being NFS-imported are mounted with the "nodev" option         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.10.2     | Ensure file systems being imported via NFS are mounted with the "nosuid" option             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.10.3     | Ensure file systems being imported via NFS are mounted with the "noexec" option             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.11.1     | Ensure nodev option set on removable media partitions                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.11.2     | Ensure nosuid option set on removable media partitions                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.11.3     | Ensure noexec option set on removable media partitions                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.12       | Ensure all non-root local partitions are mounted with the "nodev" option                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.3.1        | Ensure all information at rest is encrypted                                                 | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                      | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                      | Yes                      | No                       |
| 1.2.1.1        | Ensure GPG keys are configured                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.2        | Ensure gpgcheck is globally activated                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.3        | Ensure repo_gpgcheck is globally activated                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.4        | Ensure package manager repositories are configured                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.5        | Ensure DNF is configured to perform a signature check on local packages              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2.1        | Ensure updates, patches, and additional security software are installed              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2.2        | Ensure vendor packaged system security patches and updates are installed             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.1        | Ensure SELinux is installed                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.2        | Ensure SELinux is not disabled in bootloader configuration                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.3        | Ensure SELinux policy is configured                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.4        | Ensure the SELinux mode is not disabled                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.5        | Ensure the SELinux mode is enforcing                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.6        | Ensure no unconfined services exist                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.7        | Ensure the MCS Translation Service (mcstrans) is not installed                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.8        | Ensure the operating system has the polycoreutils package installed                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.9        | Ensure SETroubleshoot is not installed                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.10       | Ensure SELinux prevents nonprivileged users from executing privileged functions      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.1          | Ensure bootloader password is set                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.2          | Ensure access to bootloader config is configured                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.3          | Ensure the operating system requires authentication for rescue mode                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.4          | Ensure the operating system requires authentication upon booting into emergency mode | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.5          | Ensure a unique name is set as the superusers account (BIOS)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.6          | Ensure a unique name is set as the superusers account (UEFI)                         | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                     | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                     | Yes                      | No                       |
| 1.5.1          | Ensure address space layout randomization is enabled                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.2          | Ensure ptrace_scope is restricted                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.8          | Ensure the operating system enables hardening for the BPF JIT                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.10         | Ensure the NX (no-execution) bit flag is set on the system                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.11         | Ensure the operating system disables the use of user namespaces                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.13         | Ensure the operating system is configured to enable DAC on symlinks                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.15         | Ensure the operating system is configured to enable DAC on hardlinks                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.16         | Ensure the operating system restricts exposed kernel pointer addresses access                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.17         | Ensure the operating system is configured to restrict access to the kernel message buffer                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.19         | Ensure the operating system is configured to prevent kernel profiling by unprivileged users                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.20         | Ensure the operating system restricts usage of ptrace to descendant processes                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.21         | Ensure the operating system prevents privilege escalation through the kernel by disabling access to the bpf syscall | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.23         | Ensure the operating system implements the Endpoint Security for Linux Threat Prevention tool                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.1          | Ensure system wide crypto policy is not set to legacy                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.2          | Ensure system wide crypto policy is not set in sshd configuration                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.3          | Ensure system wide crypto policy disables sha1 hash and signature support                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.4          | Ensure system wide crypto policy disables macs less than 128 bits                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.5          | Ensure system wide crypto policy disables cbc for ssh                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.6          | Ensure system wide crypto policy disables chacha20-poly1305 for ssh                                                 | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                            | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                            | Yes                      | No                       |
| 1.6.7          | Ensure system wide crypto policy disables EtM for ssh                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.8          | Ensure system-wide crypto policy is FIPS                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.10         | Ensure system-wide crypto policies are in effect                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.12         | Ensure the OpenSSL library is configured to use only ciphers employing FIPS 140-2-approved algorithms                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.13         | Ensure the OpenSSL library is configured to use only DoD-approved TLS encryption                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.14         | Ensure the GnuTLS library is configured to only allow DoD-approved SSL/TLS Versions                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.4          | Ensure access to /etc/motd is configured                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.5          | Ensure access to /etc/issue is configured                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.6          | Ensure access to /etc/issue.net is configured                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.1          | Ensure GNOME Display Manager is removed                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.4          | Ensure GDM screen locks when the user is idle                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.5          | Ensure GDM screen locks cannot be overridden                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.6          | Ensure GDM automatic mounting of removable media is disabled                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.7          | Ensure GDM disabling automatic mounting of removable media is not overridden                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.8          | Ensure the operating system does not allow an unattended or automatic logon to the system via a graphical user interface   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.9          | Ensure GDM autorun-never is enabled                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.11         | Ensure GDM autorun-never is not overridden                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.12         | Ensure the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.13         | Ensure XDMCP is not enabled                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.14         | Ensure the operating system disables the user logon list for graphical user interfaces                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.16         | Ensure the operating system prevents users from overriding the session idle-delay setting for the graphical user interface | <input type="checkbox"/> | <input type="checkbox"/> |



| Recommendation |                                                                                                                                  | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                  | Yes                      | No                       |
| 1.8.17         | Ensure the operating system prevents users from overriding the screensaver lock-enabled setting for the graphical user interface | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.19         | Ensure the operating system enables a user's session lock until that user re-establishes access                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.9            | Ensure the "tmux" package installed                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.13           | Ensure the operating system has the packages required for multifactor authentication                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.1          | Ensure autofs services are not in use                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.2          | Ensure avahi daemon services are not in use                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.3          | Ensure dhcp server services are not in use                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4          | Ensure dns server services are not in use                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.5          | Ensure dnsmasq services are not in use                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.6          | Ensure ftp server services are not in use                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.7          | Ensure message access server services are not in use                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.8          | Ensure network file system services are not in use                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.9          | Ensure nis server services are not in use                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.10         | Ensure print server services are not in use                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.11         | Ensure rpcbind services are not in use                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.12         | Ensure rsync services are not in use                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.13         | Ensure samba file server services are not in use                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.14         | Ensure snmp services are not in use                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.15         | Ensure telnet server services are not in use                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.16         | Ensure tftp server services are not in use                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.17         | Ensure web proxy server services are not in use                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.18         | Ensure web server services are not in use                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.19         | Ensure xinetd services are not in use                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.20         | Ensure X window server services are not in use                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.21         | Ensure only approved services are listening on a network interface                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.22         | Ensure automated bug reporting tools are not installed                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.23         | Ensure mail transfer agents are configured for local-only mode                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                 | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                 | Yes                      | No                       |
| 2.1.24         | Ensure the sendmail package is not installed                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.25         | Ensure the rsh-server package is not installed                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.26         | Ensure system daemons are prevented from using Kerberos for authentication                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.27         | Ensure the operating system is configured to mask the debug-shell systemd service                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.28         | Ensure the gssproxy package has not been installed on the system                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.29         | Ensure the iprutils package has not been installed on the system                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.30         | Ensure the krb5-server package has not been installed on the system                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.31         | Ensure a TFTP server has not been installed on the system                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.32         | Ensure the tuned package has not been installed on the system                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.34         | Ensure the operating system is configured to prevent unrestricted mail relaying                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.1          | Ensure ftp client is not installed                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.2          | Ensure ldap client is not installed                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.3          | Ensure nis client is not installed                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.4          | Ensure telnet client is not installed                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.5          | Ensure tftp client is not installed                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.6          | Ensure krb5-workstation is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.1          | Ensure time synchronization is in use                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.2          | Ensure chrony is configured                                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.4          | Ensure the operating system is securely comparing internal information system clocks at least every 24 hours with an NTP server | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.5          | Ensure the operating system disables network management of the chrony daemon                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.6          | Ensure the operating system disables the chrony daemon from acting as a server                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.2        | Ensure permissions on /etc/crontab are configured                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                | Yes                      | No                       |
| 2.4.1.3        | Ensure permissions on /etc/cron.hourly are configured                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.4        | Ensure permissions on /etc/cron.daily are configured                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.5        | Ensure permissions on /etc/cron.weekly are configured                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.6        | Ensure permissions on /etc/cron.monthly are configured                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.7        | Ensure permissions on /etc/cron.d are configured                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.8        | Ensure crontab is restricted to authorized users                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.2.1        | Ensure at is restricted to authorized users                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5.1          | Ensure USBGuard is installed on the operating system                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5.2          | Ensure USBGuard has a policy configured                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5.3          | Ensure the operating system enables Linux audit logging of the USBGuard daemon | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5.4          | Ensure the usbguard service is enabled and active                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.6.2          | Ensure fapolicyd employs a deny-all, permit-by-exception policy                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.6.3          | Ensure fapolicyd is enabled and running                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1.1          | Ensure IPv6 status is identified                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1.2          | Ensure wireless interfaces are disabled                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1.3          | Ensure bluetooth services are not in use                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1.4          | Ensure network interfaces are not in promiscuous mode                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.1          | Ensure dccp kernel module is not available                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.2          | Ensure tipc kernel module is not available                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.3          | Ensure rds kernel module is not available                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.4          | Ensure sctp kernel module is not available                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.5          | Ensure atm kernel module is not available                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.6          | Ensure bluetooth kernel module is not available                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.7          | Ensure can kernel module is not available                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.1          | Ensure ip forwarding is disabled                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.2          | Ensure packet redirect sending is disabled                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.3          | Ensure bogus icmp responses are ignored                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.4          | Ensure broadcast icmp requests are ignored                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.5          | Ensure icmp redirects are not accepted                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.6          | Ensure secure icmp redirects are not accepted                                  | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                            | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                            | Yes                      | No                       |
| 3.3.7          | Ensure reverse path filtering is enabled                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.8          | Ensure source routed packets are not accepted                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.9          | Ensure suspicious packets are logged                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.10         | Ensure tcp syn cookies is enabled                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.11         | Ensure ipv6 router advertisements are not accepted                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.12         | Ensure net.ipv4.conf.all.forwarding is disabled                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.1        | Ensure nftables base chains exist                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.2        | Ensure host based firewall loopback traffic is configured                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.3        | Ensure firewalld drops unnecessary services and ports                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.4        | Ensure nftables established connections are configured                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.5        | Ensure nftables default deny firewall policy                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2          | Ensure the firewall is configured to remove unnecessary use of functions, ports, protocols, and/or services                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.3          | Ensure firewalld service is enabled and running                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.4          | Ensure nftables is installed                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.5          | Ensure a single firewall configuration utility is in use                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.6          | Ensure "nftables" is configured to allow rate limits on any connection to the system                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.7          | Ensure "firewalld" is installed                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.8          | Ensure "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1          | Ensure openssh-server is installed                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2          | Ensure permissions on /etc/ssh/sshd_config are configured                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3          | Ensure permissions on SSH private host key files are configured                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.4          | Ensure permissions on SSH public host key files are configured                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.5          | Ensure sshd access is configured                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.7          | Ensure sshd Ciphers are configured                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.9          | Ensure sshd DisableForwarding is enabled                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.10         | Ensure sshd GSSAPIAuthentication is disabled                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                  | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                  | Yes                      | No                       |
| 5.1.12         | Ensure sshd IgnoreRhosts is enabled                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.13         | Ensure sshd KexAlgorithms is configured                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.15         | Ensure sshd LogLevel is configured                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.16         | Ensure sshd MACs are configured                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.17         | Ensure sshd MaxAuthTries is configured                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.20         | Ensure sshd PermitEmptyPasswords is disabled                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.21         | Ensure sshd PermitRootLogin is disabled                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.23         | Ensure sshd UsePAM is enabled                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.24         | Ensure sshd private key files have a passcode                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.25         | Ensure sshd X11Forwarding is disabled                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.26         | Ensure sshd ClientAliveInterval is configured                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.27         | Ensure sshd ClientAliveCountMax is configured                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.28         | Ensure the SSH server is configured to use only MACs employing FIPS 140-2-approved algorithms    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.29         | Ensure the SSH server is configured to use only ciphers employing FIPS 140-2-approved algorithms | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.30         | Ensure sshd is configured to use only FIPS-validated key exchange algorithms                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.31         | Ensure the SSH server uses strong entropy                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.34         | Ensure sshd IgnoreUserKnownHosts is enabled                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.36         | Ensure sshd KerberosAuthentication is disabled                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.37         | Ensure sshd RekeyLimit is configured                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.39         | Ensure SSH is loaded and active                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1          | Ensure sudo is installed                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2          | Ensure the sudoers file has the default include directory                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3          | Ensure sudo commands use pty                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4          | Ensure sudo log file exists                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.5          | Ensure users must provide password for escalation                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.6          | Ensure the sudoers file restricts sudo access to authorized personnel                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.7          | Ensure re-authentication for privilege escalation is not disabled globally                       | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                               | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                               | Yes                      | No                       |
| 5.2.8          | Ensure the sudoers security policy is configured to use the invoking user's password for privilege escalation | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.9          | Ensure sudo timestamp_timeout is configured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.10         | Ensure access to the su command is restricted                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.11         | Ensure pam_succeed_if does not exist in /etc/pam.d/sudo                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.1        | Ensure active authselect profile includes pam modules                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.2        | Ensure pam_faillock module is enabled                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.3        | Ensure pam_pwquality module is enabled                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.4        | Ensure pam_pwhistory module is enabled                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.1      | Ensure password failed attempts lockout is configured                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.2      | Ensure password unlock time is configured                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.3      | Ensure password failed attempts lockout includes root account                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.4      | Ensure deny is configured on the pam_faillock module                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.5      | Ensure deny is configured in /etc/security/faillock.conf                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.6      | Ensure fail_interval is configured on the pam_faillock module                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.7      | Ensure fail_interval is configured in /etc/security/faillock.conf                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.8      | Ensure unlock_time is configured on the pam_faillock module                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.9      | Ensure unlock_time is configured in /etc/security/faillock.conf                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.10     | Ensure dir is configured on the pam_faillock module                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.11     | Ensure dir is configured in /etc/security/faillock.conf                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.14     | Ensure audit is set on the pam_faillock module                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.15     | Ensure audit is set in /etc/security/faillock.conf                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.16     | Ensure even_deny_root is set on the pam_faillock module                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.17     | Ensure even_deny_root is set in /etc/security/faillock.conf                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.18     | Ensure the use of a non-default faillock tally directory while SELinux enforces a targeted policy             | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                              | Set Correctly            |                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                              | Yes                      | No                       |
| 5.3.3.1.19     | Ensure the use of a non-default faillock tally directory on the pam_faillock module while SELinux enforces a targeted policy | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.1      | Ensure password number of changed characters is configured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.2      | Ensure password length is configured                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.3      | Ensure password complexity is configured                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.4      | Ensure password same consecutive characters is configured                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.5      | Ensure password maximum sequential characters is configured                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.6      | Ensure password dictionary check is enabled                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.7      | Ensure password quality is enforced for the root user                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.8      | Ensure the operating system enforces a minimum 15-character password length                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.9      | Ensure ucredit is configured in /etc/security/pwquality.conf                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.10     | Ensure lcredit is configured in /etc/security/pwquality.conf                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.11     | Ensure dcredit is configured in /etc/security/pwquality.conf                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.12     | Ensure ocredit is configured in /etc/security/pwquality.conf                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.13     | Ensure maxclassrepeat is configured in /etc/security/pwquality.conf                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.14     | Ensure minclass is configured in /etc/security/pwquality.conf                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.15     | Ensure difok is configured in /etc/security/pwquality.conf                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.16     | Ensure dictcheck is configured                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.17     | Ensure retry is configured on the pam_pwquality module in /etc/pam.d/system-auth                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.18     | Ensure retry is configured on the pam_pwquality module in /etc/pam.d/password-auth                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.19     | Ensure retry is configured in /etc/security/pwquality.conf                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.1      | Ensure password history remember is configured                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.2      | Ensure password history is enforced for the root user                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                  | Set Correctly            |                          |
|----------------|------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                  | Yes                      | No                       |
| 5.3.3.3.3      | Ensure pam_pwhistory includes use_authok                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.5      | Ensure remember is configured on the pam_pwhistory module in /etc/pam.d/system-auth                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.1      | Ensure pam_unix does not include nullok                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.2      | Ensure pam_unix does not include remember                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.3      | Ensure pam_unix includes a strong password hashing algorithm                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.4      | Ensure pam_unix includes use_authok                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.5      | Ensure pam_unix includes a FIPS 140-2 approved hashing algorithm                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.6.1      | Ensure the operating system uses multifactor authentication for local access to accounts                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.6.3      | Ensure the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.1        | Ensure password expiration is configured                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.2        | Ensure minimum password days is configured                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.3        | Ensure password expiration warning days is configured                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.4        | Ensure strong password hashing algorithm is configured                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.5        | Ensure inactive password lock is configured                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.6        | Ensure all users last password change date is in the past                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.7        | Ensure passwords use FIPS 140-2 approved cryptographic hashing algorithm                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.8        | Ensure minimum number of hashing rounds is configured                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.9        | Ensure existing passwords use FIPS 140-2 approved cryptographic hashing algorithm                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.12       | Ensure pass_min_len is configured                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.13       | Ensure the maximum time period for existing passwords is restricted to 60 days                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.2        | Ensure root is the only GID 0 account                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.3        | Ensure group root is the only GID 0 group                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.4        | Ensure root account access is controlled                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.6        | Ensure root user umask is configured                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.7        | Ensure system accounts do not have a valid login shell                                                           | <input type="checkbox"/> | <input type="checkbox"/> |



| Recommendation |                                                                                                                                                          | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                          | Yes                      | No                       |
| 5.4.2.8        | Ensure accounts without a valid login shell are locked                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.2        | Ensure default user shell timeout is configured                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.3        | Ensure default user umask is configured                                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.5        | Ensure the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.6        | Ensure the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.7        | Ensure the operating system enforces a 60-day maximum password lifetime for new user accounts                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.8        | Ensure the umask default for installed shells is "077"                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.9        | Ensure the default umask for all local interactive users is "077"                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.10       | Ensure the operating system initiates a session lock after 15 minutes of inactivity                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.11       | Ensure the operating system prevents users from disabling the tmux terminal multiplexer                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.12       | Ensure the operating system's shell initialization file is configured to start each shell with the tmux terminal multiplexer                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.13       | Ensure the operating system enables the user to initiate a session lock                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.16       | Ensure StopIdleSessionSec is configured                                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.1          | Ensure AIDE is installed                                                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.2          | Ensure filesystem integrity is regularly checked                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.4          | Ensure AIDE is configured to use cryptographic mechanisms to protect the integrity of audit tools                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.5          | Ensure the file integrity tool is configured to verify ACLs                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.6          | Ensure the file integrity tool is configured to verify extended attributes                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.1      | Ensure journald service is enabled and active                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.2      | Ensure journald log file access is configured                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.3      | Ensure journald log file rotation is configured                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.4      | Ensure journald ForwardToSyslog is disabled                                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                              | Set Correctly            |                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                              | Yes                      | No                       |
| 6.2.1.1.5      | Ensure journald Storage is configured                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.6      | Ensure journald Compress is configured                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.1      | Ensure systemd-journal-remote is installed                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.2      | Ensure systemd-journal-remote authentication is configured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.3      | Ensure systemd-journal-upload is enabled and active                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.4      | Ensure systemd-journal-remote service is not in use                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.1        | Ensure rsyslog is installed                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.2        | Ensure rsyslog service is enabled and active                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.3        | Ensure all remote access methods are monitored                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.4        | Ensure journald is configured to send logs to rsyslog                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.5        | Ensure rsyslog log file creation mode is configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.6        | Ensure rsyslog logging is configured                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.7        | Ensure rsyslog is configured to send logs to a remote log host                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.8        | Ensure rsyslog is not configured to receive logs from a remote client                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.9        | Ensure logrotate is configured                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.10       | Ensure rsyslog is configured to log cron events                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.11       | Ensure the rsyslog service is enabled and active                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.12       | Ensure the operating system has the packages required for encrypting offloaded audit logs                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.13       | Ensure the the operating system authenticates the remote logging server for off-loading audit logs                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.14       | Ensure the operating system encrypts audit records off-loaded onto a different system or media from the system being audited | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.15       | Ensure the audit system off-loads audit records onto a different system or media from the system being audited               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.1        | Ensure access to all logfiles has been configured                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.2        | Ensure /var/log/messages mode is configured                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.3        | Ensure /var/log/messages owner is configured                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.4        | Ensure /var/log/messages group owner is configured                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                                                | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                                | Yes                      | No                       |
| 6.2.3.5        | Ensure /var/log is mode is configured                                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.6        | Ensure /var/log owner is configured                                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.7        | Ensure /var/log group owner is configured                                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.8        | Ensure administrators are notified if an audit processing failure occurs by modifying /etc/aliases                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.1        | Ensure auditd packages are installed                                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.2        | Ensure auditing for processes that start prior to auditd is enabled                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.3        | Ensure audit_backlog_limit is sufficient                                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.4        | Ensure auditd service is enabled and active                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.5        | Ensure the operating system allocates a sufficient audit_backlog_limit to capture processes that start prior to the audit daemon                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.6        | Ensure the operating system's audit daemon is configured to include local events                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.7        | Ensure the operating system's audit daemon is configured to label all off-loaded audit logs                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.8        | Ensure the operating system's audit daemon is configured to resolve audit information before writing to disk                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.1        | Ensure audit log storage size is configured                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.2        | Ensure audit logs are not automatically deleted                                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.5        | Ensure the operating system allocates audit record storage capacity                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.6        | Ensure the SA and ISSO are notified in the event of an audit processing failure                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.7        | Ensure the operating system notifies the SA and ISSO when allocated audit record storage volume reaches 75 percent                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.8        | Ensure the operating system takes action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.9        | Ensure the audit system is configured to take an appropriate action when the internal event queue is full                                                      | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                      | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                      | Yes                      | No                       |
| 6.3.3.1        | Ensure changes to system administration scope (sudoers) is collected                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.2        | Ensure actions as another user are always logged                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.3        | Ensure events that modify the sudo log file are collected                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.4        | Ensure events that modify date and time information are collected                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.5        | Ensure events that modify the system's network environment are collected             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.6        | Ensure use of privileged commands are collected                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.7        | Ensure unsuccessful file access attempts are collected                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.8        | Ensure events that modify user/group information are collected                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.9        | Ensure discretionary access control permission modification events are collected     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.10       | Ensure successful file system mounts are collected                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.11       | Ensure session initiation information is collected                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.12       | Ensure login and logout events are collected                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.13       | Ensure file deletion events by users are collected                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.14       | Ensure events that modify the system's Mandatory Access Controls are collected       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.15       | Ensure successful and unsuccessful attempts to use the chcon command are collected   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.16       | Ensure successful and unsuccessful attempts to use the setfacl command are collected | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.17       | Ensure successful and unsuccessful attempts to use the chacl command are collected   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.18       | Ensure successful and unsuccessful attempts to use the usermod command are collected | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.19       | Ensure kernel module loading unloading and modification is collected                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.20       | Ensure the audit configuration is immutable                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.21       | Ensure the running and on disk configuration is the same                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.22       | Ensure successful and unsuccessful attempts to use the su command are collected      | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                  | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                  | Yes                      | No                       |
| 6.3.3.23       | Ensure successful and unsuccessful attempts to use the sudo command are collected                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.24       | Ensure successful and unsuccessful attempts to use the chsh command are collected                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.25       | Ensure successful and unsuccessful attempts to use the crontab command are collected             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.26       | Ensure successful and unsuccessful attempts to use the gpasswd command are collected             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.27       | Ensure successful and unsuccessful attempts to use the newgrp command are collected              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.28       | Ensure successful and unsuccessful attempts to use the pam_timestamp_check command are collected | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.29       | Ensure successful and unsuccessful attempts to use the ssh-keysign command are collected         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.30       | Ensure successful and unsuccessful attempts to use the unix_chkpwd command are collected         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.31       | Ensure successful and unsuccessful attempts to use the setsebool command are collected           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.32       | Ensure successful and unsuccessful attempts to use the userhelper command are collected          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.33       | Ensure successful and unsuccessful attempts to use the setfiles command are collected            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.34       | Ensure successful and unsuccessful attempts to use the semanage command are collected            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.35       | Ensure successful and unsuccessful attempts to use the postqueue command are collected           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.36       | Ensure successful and unsuccessful attempts to use the postdrop command are collected            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.37       | Ensure successful and unsuccessful attempts to use the unix_update command are collected         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.38       | Ensure successful and unsuccessful attempts to use the umount command are collected              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.39       | Ensure successful and unsuccessful attempts to use the mount command are collected               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.40       | Ensure successful and unsuccessful attempts to use the ssh-agent command are collected           | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                     | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                     | Yes                      | No                       |
| 6.3.3.41       | Ensure successful and unsuccessful attempts to use the passwd command are collected | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.42       | Ensure successful and unsuccessful attempts to use the chage command are collected  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.43       | Ensure the audit system prevents unauthorized changes to logon UIDs                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.44       | Ensure successful and unsuccessful modifications to the faillock file are collected | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.1        | Ensure the audit log file directory mode is configured                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.2        | Ensure audit log files mode is configured                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.3        | Ensure audit log files owner is configured                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.4        | Ensure audit log files group owner is configured                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.5        | Ensure audit configuration files mode is configured                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.6        | Ensure audit configuration files owner is configured                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.7        | Ensure audit configuration files group owner is configured                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.8        | Ensure audit tools mode is configured                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.9        | Ensure audit tools owner is configured                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.10       | Ensure audit tools group owner is configured                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.11       | Ensure the audit logs are group-owned by root                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.12       | Ensure audit tools are mode 0755 or more restrictive                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.13       | Ensure the audit tools are owned by root                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.14       | Ensure audit tools are group owned by root                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.15       | Ensure the audit log file directories are mode 0700 or more restrictive             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.16       | Ensure the audit log file directory is owned by root                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.17       | Ensure audit log files group owner is root                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.18       | Ensure audit log files are mode 0600 or more restrictive                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.1          | Ensure permissions on /etc/passwd are configured                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.2          | Ensure permissions on /etc/passwd- are configured                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.3          | Ensure permissions on /etc/group are configured                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.4          | Ensure permissions on /etc/group- are configured                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.5          | Ensure permissions on /etc/shadow are configured                                    | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                           | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                           | Yes                      | No                       |
| 7.1.6          | Ensure permissions on /etc/shadow- are configured                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.7          | Ensure permissions on /etc/gshadow are configured                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.8          | Ensure permissions on /etc/gshadow- are configured                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.9          | Ensure permissions on /etc/shells are configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.10         | Ensure permissions on /etc/security/opasswd are configured                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.11         | Ensure world writable files and directories are secured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.12         | Ensure no files or directories without an owner and a group exist                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.13         | Ensure SUID and SGID files are reviewed                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.14         | Ensure there are no ".shosts" files on the operating system                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.15         | Ensure there are no "shosts.equiv" files on the operating system                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.16         | Ensure system-wide shared library directories have mode 755 or less permissive                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.17         | Ensure system-wide shared library directories must be owned by root                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.18         | Ensure the system-wide shared library directories are group-owned by root or a system account                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.19         | Ensure world-writable directories owner is configured                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.20         | Ensure world-writable directories group-owner is configured                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.21         | Ensure local initialization files do not execute world-writable programs                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.22         | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are mode 0755 or more restrictive | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.23         | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are owned by root                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.24         | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are group-owned by root           | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.25         | Ensure the system-wide shared library files are mode 0755 or more restrictive                                             | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                       | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                       | Yes                      | No                       |
| 7.1.26         | Ensure the system-wide shared library files are owned by root                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.27         | Ensure the system-wide shared library files are group-owned by root                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.1          | Ensure accounts in /etc/passwd use shadowed passwords                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.2          | Ensure /etc/shadow password fields are not empty                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.4          | Ensure shadow group is empty                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.9          | Ensure local interactive user home directories are configured                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.10         | Ensure local interactive user dot files access is configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.11         | Ensure all files and directories in the local interactive user home directory are group-owned by a group that the user is a member of | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.12         | Ensure all files and directories in a local interactive user home directory are mode 0750 or more restrictive                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.13         | Ensure all local initialization files are mode 0740 or more restrictive                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.14         | Ensure local interactive user home directories group-owner is their primary GID                                                       | <input type="checkbox"/> | <input type="checkbox"/> |



# Appendix: CIS Controls v7 Unmapped Recommendations

| Recommendation |                                                                                                                             | Set Correctly            |                          |
|----------------|-----------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                             | Yes                      | No                       |
| 1.2.2.3        | Ensure Operating System is a vendor-supported release                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.11       | Ensure SELinux targeted policy is configured                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.1          | Ensure message of the day is configured properly                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.2          | Ensure local login warning banner is configured properly                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.3          | Ensure remote login warning banner is configured properly                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.2          | Ensure GDM login banner is configured                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.3          | Ensure GDM disable-user-list option is enabled                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.18         | Ensure the operating system initiates a session lock for all connection types using smartcard when the smartcard is removed | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.3          | Ensure chrony is not run as the root user                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.1        | Ensure cron daemon is enabled and active                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.6          | Ensure sshd Banner is configured                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.8          | Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.11         | Ensure sshd HostbasedAuthentication is disabled                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.14         | Ensure sshd LoginGraceTime is configured                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.18         | Ensure sshd MaxSessions is configured                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.19         | Ensure sshd MaxStartups is configured                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.22         | Ensure sshd PermitUserEnvironment is disabled                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.33         | Ensure sshd Banner is configured to display the Standard Mandatory DoD Notice and Consent Banner                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.1.1        | Ensure latest version of pam is installed                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.1.2        | Ensure latest version of authselect is installed                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.5        | Ensure pam_unix module is enabled                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.1        | Ensure root is the only UID 0 account                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.5        | Ensure root path integrity                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                  | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                  | Yes                      | No                       |
| 5.4.3.1        | Ensure nologin is not listed in /etc/shells                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.3          | Ensure cryptographic mechanisms are used to protect the integrity of audit tools | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.3        | Ensure system is disabled when audit logs are full                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.4        | Ensure system warns when audit logs are low on space                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.3          | Ensure all groups in /etc/passwd exist in /etc/group                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.5          | Ensure no duplicate UIDs exist                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.6          | Ensure no duplicate GIDs exist                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.7          | Ensure no duplicate user names exist                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.8          | Ensure no duplicate group names exist                                            | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: CIS Controls v8 IG 1 Mapped Recommendations

| Recommendation |                                                                                             | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                             | Yes                      | No                       |
| 1.1.1.9        | Ensure usb-storage kernel module is not available                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.3      | Ensure nosuid option set on /tmp partition                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.4      | Ensure noexec option set on /tmp partition                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.2      | Ensure nodev option set on /dev/shm partition                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.3      | Ensure nosuid option set on /dev/shm partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.4      | Ensure noexec option set on /dev/shm partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.1      | Ensure separate partition exists for /home                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.2      | Ensure nodev option set on /home partition                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.3      | Ensure nosuid option set on /home partition                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.5      | Ensure file systems that contain user home directories are mounted with the nosuid option   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.6      | Ensure file systems that contain user home directories are mounted with the "noexec" option | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.4.1      | Ensure separate partition exists for /var                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.4.2      | Ensure nodev option set on /var partition                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.4.3      | Ensure nosuid option set on /var partition                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.1      | Ensure separate partition exists for /var/tmp                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.2      | Ensure nodev option set on /var/tmp partition                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.3      | Ensure nosuid option set on /var/tmp partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.4      | Ensure noexec option set on /var/tmp partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.1      | Ensure separate partition exists for /var/log                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.2      | Ensure nodev option set on /var/log partition                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.3      | Ensure nosuid option set on /var/log partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.4      | Ensure noexec option set on /var/log partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.1      | Ensure separate partition exists for /var/log/audit                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.2      | Ensure nodev option set on /var/log/audit partition                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.3      | Ensure nosuid option set on /var/log/audit partition                                        | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                     | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                     | Yes                      | No                       |
| 1.1.2.7.4      | Ensure noexec option set on /var/log/audit partition                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.8.1      | Ensure the "/boot" directory is mounted with the "nosuid" option                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.9.1      | Ensure the "/boot/efi" directory is mounted with the "nosuid" option                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.10.1     | Ensure file systems that are being NFS-imported are mounted with the "nodev" option | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.10.2     | Ensure file systems being imported via NFS are mounted with the "nosuid" option     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.10.3     | Ensure file systems being imported via NFS are mounted with the "noexec" option     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.11.1     | Ensure nodev option set on removable media partitions                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.11.2     | Ensure nosuid option set on removable media partitions                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.11.3     | Ensure noexec option set on removable media partitions                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.12       | Ensure all non-root local partitions are mounted with the "nodev" option            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.1        | Ensure GPG keys are configured                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.2        | Ensure gpgcheck is globally activated                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.3        | Ensure repo_gpgcheck is globally activated                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.4        | Ensure package manager repositories are configured                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.5        | Ensure DNF is configured to perform a signature check on local packages             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2.1        | Ensure updates, patches, and additional security software are installed             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2.2        | Ensure vendor packaged system security patches and updates are installed            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.1        | Ensure SELinux is installed                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.2        | Ensure SELinux is not disabled in bootloader configuration                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.3        | Ensure SELinux policy is configured                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.4        | Ensure the SELinux mode is not disabled                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.5        | Ensure the SELinux mode is enforcing                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.6        | Ensure no unconfined services exist                                                 | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                     | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                     | Yes                      | No                       |
| 1.3.1.8        | Ensure the operating system has the policycoreutils package installed                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.10       | Ensure SELinux prevents nonprivileged users from executing privileged functions                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.11       | Ensure SELinux targeted policy is configured                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.1          | Ensure bootloader password is set                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.2          | Ensure access to bootloader config is configured                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.3          | Ensure the operating system requires authentication for rescue mode                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.4          | Ensure the operating system requires authentication upon booting into emergency mode                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.5          | Ensure a unique name is set as the superusers account (BIOS)                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.6          | Ensure a unique name is set as the superusers account (UEFI)                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.13         | Ensure the operating system is configured to enable DAC on symlinks                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.15         | Ensure the operating system is configured to enable DAC on hardlinks                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.17         | Ensure the operating system is configured to restrict access to the kernel message buffer                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.19         | Ensure the operating system is configured to prevent kernel profiling by unprivileged users                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.21         | Ensure the operating system prevents privilege escalation through the kernel by disabling access to the bpf syscall | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.4          | Ensure access to /etc/motd is configured                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.5          | Ensure access to /etc/issue is configured                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.6          | Ensure access to /etc/issue.net is configured                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.4          | Ensure GDM screen locks when the user is idle                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.5          | Ensure GDM screen locks cannot be overridden                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.6          | Ensure GDM automatic mounting of removable media is disabled                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.7          | Ensure GDM disabling automatic mounting of removable media is not overridden                                        | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                  | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                  | Yes                      | No                       |
| 1.8.8          | Ensure the operating system does not allow an unattended or automatic logon to the system via a graphical user interface         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.9          | Ensure GDM autorun-never is enabled                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.11         | Ensure GDM autorun-never is not overridden                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.12         | Ensure the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.14         | Ensure the operating system disables the user logon list for graphical user interfaces                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.16         | Ensure the operating system prevents users from overriding the session idle-delay setting for the graphical user interface       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.17         | Ensure the operating system prevents users from overriding the screensaver lock-enabled setting for the graphical user interface | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.18         | Ensure the operating system initiates a session lock for all connection types using smartcard when the smartcard is removed      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.19         | Ensure the operating system enables a user's session lock until that user re-establishes access                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.9            | Ensure the "tmux" package installed                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.13           | Ensure the operating system has the packages required for multifactor authentication                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.1          | Ensure autofs services are not in use                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.2        | Ensure permissions on /etc/crontab are configured                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.3        | Ensure permissions on /etc/cron.hourly are configured                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.4        | Ensure permissions on /etc/cron.daily are configured                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.5        | Ensure permissions on /etc/cron.weekly are configured                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.6        | Ensure permissions on /etc/cron.monthly are configured                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.7        | Ensure permissions on /etc/cron.d are configured                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.8        | Ensure crontab is restricted to authorized users                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.2.1        | Ensure at is restricted to authorized users                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5.1          | Ensure USBGuard is installed on the operating system                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.1        | Ensure nftables base chains exist                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                            | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                            | Yes                      | No                       |
| 4.1.1.2        | Ensure host based firewall loopback traffic is configured                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.3        | Ensure firewalld drops unnecessary services and ports                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.4        | Ensure nftables established connections are configured                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.5        | Ensure nftables default deny firewall policy                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2          | Ensure the firewall is configured to remove unnecessary use of functions, ports, protocols, and/or services                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.3          | Ensure firewalld service is enabled and running                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.4          | Ensure nftables is installed                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.5          | Ensure a single firewall configuration utility is in use                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.6          | Ensure "nftables" is configured to allow rate limits on any connection to the system                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.7          | Ensure "firewalld" is installed                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.8          | Ensure "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2          | Ensure permissions on /etc/ssh/sshd_config are configured                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3          | Ensure permissions on SSH private host key files are configured                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.4          | Ensure permissions on SSH public host key files are configured                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.5          | Ensure sshd access is configured                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.10         | Ensure sshd GSSAPIAuthentication is disabled                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.12         | Ensure sshd IgnoreRhosts is enabled                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.15         | Ensure sshd LogLevel is configured                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.20         | Ensure sshd PermitEmptyPasswords is disabled                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.21         | Ensure sshd PermitRootLogin is disabled                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.23         | Ensure sshd UsePAM is enabled                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.24         | Ensure sshd private key files have a passcode                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.26         | Ensure sshd ClientAliveInterval is configured                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.27         | Ensure sshd ClientAliveCountMax is configured                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.28         | Ensure the SSH server is configured to use only MACs employing FIPS 140-2-approved algorithms                              | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                               | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                               | Yes                      | No                       |
| 5.1.34         | Ensure sshd IgnoreUserKnownHosts is enabled                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1          | Ensure sudo is installed                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2          | Ensure the sudoers file has the default include directory                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3          | Ensure sudo commands use pty                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.5          | Ensure users must provide password for escalation                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.6          | Ensure the sudoers file restricts sudo access to authorized personnel                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.7          | Ensure re-authentication for privilege escalation is not disabled globally                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.8          | Ensure the sudoers security policy is configured to use the invoking user's password for privilege escalation | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.9          | Ensure sudo timestamp_timeout is configured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.10         | Ensure access to the su command is restricted                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.11         | Ensure pam_succeed_if does not exist in /etc/pam.d/sudo                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.2        | Ensure pam_faillock module is enabled                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.3        | Ensure pam_pwquality module is enabled                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.4        | Ensure pam_pwhistory module is enabled                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.1      | Ensure password failed attempts lockout is configured                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.2      | Ensure password unlock time is configured                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.3      | Ensure password failed attempts lockout includes root account                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.4      | Ensure deny is configured on the pam_faillock module                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.5      | Ensure deny is configured in /etc/security/faillock.conf                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.6      | Ensure fail_interval is configured on the pam_faillock module                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.7      | Ensure fail_interval is configured in /etc/security/faillock.conf                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.8      | Ensure unlock_time is configured on the pam_faillock module                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.9      | Ensure unlock_time is configured in /etc/security/faillock.conf                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.10     | Ensure dir is configured on the pam_faillock module                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.11     | Ensure dir is configured in /etc/security/faillock.conf                                                       | <input type="checkbox"/> | <input type="checkbox"/> |



| Recommendation |                                                                                                                              | Set Correctly            |                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                              | Yes                      | No                       |
| 5.3.3.1.16     | Ensure even_deny_root is set on the pam_faillock module                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.17     | Ensure even_deny_root is set in /etc/security/faillock.conf                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.18     | Ensure the use of a non-default faillock tally directory while SELinux enforces a targeted policy                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.19     | Ensure the use of a non-default faillock tally directory on the pam_faillock module while SELinux enforces a targeted policy | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.1      | Ensure password number of changed characters is configured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.2      | Ensure password length is configured                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.3      | Ensure password complexity is configured                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.4      | Ensure password same consecutive characters is configured                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.5      | Ensure password maximum sequential characters is configured                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.6      | Ensure password dictionary check is enabled                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.7      | Ensure password quality is enforced for the root user                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.8      | Ensure the operating system enforces a minimum 15-character password length                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.9      | Ensure ucredit is configured in /etc/security/pwquality.conf                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.10     | Ensure lcredit is configured in /etc/security/pwquality.conf                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.11     | Ensure dcredit is configured in /etc/security/pwquality.conf                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.12     | Ensure ocredit is configured in /etc/security/pwquality.conf                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.13     | Ensure maxclassrepeat is configured in /etc/security/pwquality.conf                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.14     | Ensure minclass is configured in /etc/security/pwquality.conf                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.15     | Ensure difok is configured in /etc/security/pwquality.conf                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.16     | Ensure dictcheck is configured                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.17     | Ensure retry is configured on the pam_pwquality module in /etc/pam.d/system-auth                                             | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                   | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                   | Yes                      | No                       |
| 5.3.3.2.18     | Ensure retry is configured on the pam_pwquality module in /etc/pam.d/password-auth                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.19     | Ensure retry is configured in /etc/security/pwquality.conf                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.1      | Ensure password history remember is configured                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.2      | Ensure password history is enforced for the root user                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.4      | Ensure remember is configured on the pam_pwhistory module in /etc/pam.d/password-auth                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.5      | Ensure remember is configured on the pam_pwhistory module in /etc/pam.d/system-auth                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.1      | Ensure pam_unix does not include nullok                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.2      | Ensure pam_unix does not include remember                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.6.1      | Ensure the operating system uses multifactor authentication for local access to accounts                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.6.3      | Ensure the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.1        | Ensure password expiration is configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.2        | Ensure minimum password days is configured                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.3        | Ensure password expiration warning days is configured                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.5        | Ensure inactive password lock is configured                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.6        | Ensure all users last password change date is in the past                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.12       | Ensure pass_min_len is configured                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.13       | Ensure the maximum time period for existing passwords is restricted to 60 days                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.2        | Ensure root is the only GID 0 account                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.3        | Ensure group root is the only GID 0 group                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.4        | Ensure root account access is controlled                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.6        | Ensure root user umask is configured                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.7        | Ensure system accounts do not have a valid login shell                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.8        | Ensure accounts without a valid login shell are locked                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.2        | Ensure default user shell timeout is configured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.3        | Ensure default user umask is configured                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.5        | Ensure the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                                          | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                          | Yes                      | No                       |
| 5.4.3.6        | Ensure the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.7        | Ensure the operating system enforces a 60-day maximum password lifetime for new user accounts                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.8        | Ensure the umask default for installed shells is "077"                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.9        | Ensure the default umask for all local interactive users is "077"                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.10       | Ensure the operating system initiates a session lock after 15 minutes of inactivity                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.11       | Ensure the operating system prevents users from disabling the tmux terminal multiplexer                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.12       | Ensure the operating system's shell initialization file is configured to start each shell with the tmux terminal multiplexer                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.13       | Ensure the operating system enables the user to initiate a session lock                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.16       | Ensure StopIdleSessionSec is configured                                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.1      | Ensure journald service is enabled and active                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.2      | Ensure journald log file access is configured                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.3      | Ensure journald log file rotation is configured                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.4      | Ensure journald ForwardToSyslog is disabled                                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.5      | Ensure journald Storage is configured                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.6      | Ensure journald Compress is configured                                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.1      | Ensure systemd-journal-remote is installed                                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.2      | Ensure systemd-journal-remote authentication is configured                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.3      | Ensure systemd-journal-upload is enabled and active                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.1        | Ensure rsyslog is installed                                                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.2        | Ensure rsyslog service is enabled and active                                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.3        | Ensure all remote access methods are monitored                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.4        | Ensure journald is configured to send logs to rsyslog                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.5        | Ensure rsyslog log file creation mode is configured                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.6        | Ensure rsyslog logging is configured                                                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                                                | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                                | Yes                      | No                       |
| 6.2.2.7        | Ensure rsyslog is configured to send logs to a remote log host                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.9        | Ensure logrotate is configured                                                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.11       | Ensure the rsyslog service is enabled and active                                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.1        | Ensure access to all logfiles has been configured                                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.2        | Ensure /var/log/messages mode is configured                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.3        | Ensure /var/log/messages owner is configured                                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.4        | Ensure /var/log/messages group owner is configured                                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.5        | Ensure /var/log is mode is configured                                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.6        | Ensure /var/log owner is configured                                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.7        | Ensure /var/log group owner is configured                                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.8        | Ensure administrators are notified if an audit processing failure occurs by modifying /etc/aliases                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.1        | Ensure auditd packages are installed                                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.2        | Ensure auditing for processes that start prior to auditd is enabled                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.3        | Ensure audit_backlog_limit is sufficient                                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.4        | Ensure auditd service is enabled and active                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.1        | Ensure audit log storage size is configured                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.2        | Ensure audit logs are not automatically deleted                                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.3        | Ensure system is disabled when audit logs are full                                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.4        | Ensure system warns when audit logs are low on space                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.5        | Ensure the operating system allocates audit record storage capacity                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.6        | Ensure the SA and ISSO are notified in the event of an audit processing failure                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.7        | Ensure the operating system notifies the SA and ISSO when allocated audit record storage volume reaches 75 percent                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.8        | Ensure the operating system takes action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.9        | Ensure the audit system is configured to take an appropriate action when the internal event queue is full                                                      | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                      | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                      | Yes                      | No                       |
| 6.3.3.15       | Ensure successful and unsuccessful attempts to use the chcon command are collected   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.16       | Ensure successful and unsuccessful attempts to use the setfacl command are collected | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.17       | Ensure successful and unsuccessful attempts to use the chacl command are collected   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.18       | Ensure successful and unsuccessful attempts to use the usermod command are collected | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.20       | Ensure the audit configuration is immutable                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.1        | Ensure the audit log file directory mode is configured                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.2        | Ensure audit log files mode is configured                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.3        | Ensure audit log files owner is configured                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.4        | Ensure audit log files group owner is configured                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.5        | Ensure audit configuration files mode is configured                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.6        | Ensure audit configuration files owner is configured                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.7        | Ensure audit configuration files group owner is configured                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.8        | Ensure audit tools mode is configured                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.9        | Ensure audit tools owner is configured                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.10       | Ensure audit tools group owner is configured                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.11       | Ensure the audit logs are group-owned by root                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.12       | Ensure audit tools are mode 0755 or more restrictive                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.13       | Ensure the audit tools are owned by root                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.14       | Ensure audit tools are group owned by root                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.15       | Ensure the audit log file directories are mode 0700 or more restrictive              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.16       | Ensure the audit log file directory is owned by root                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.17       | Ensure audit log files group owner is root                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.18       | Ensure audit log files are mode 0600 or more restrictive                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.1          | Ensure permissions on /etc/passwd are configured                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.2          | Ensure permissions on /etc/passwd- are configured                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.3          | Ensure permissions on /etc/group are configured                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.4          | Ensure permissions on /etc/group- are configured                                     | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                           | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                           | Yes                      | No                       |
| 7.1.5          | Ensure permissions on /etc/shadow are configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.6          | Ensure permissions on /etc/shadow- are configured                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.7          | Ensure permissions on /etc/gshadow are configured                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.8          | Ensure permissions on /etc/gshadow- are configured                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.9          | Ensure permissions on /etc/shells are configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.10         | Ensure permissions on /etc/security/opasswd are configured                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.11         | Ensure world writable files and directories are secured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.12         | Ensure no files or directories without an owner and a group exist                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.13         | Ensure SUID and SGID files are reviewed                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.14         | Ensure there are no ".shosts" files on the operating system                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.15         | Ensure there are no "shosts.equiv" files on the operating system                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.16         | Ensure system-wide shared library directories have mode 755 or less permissive                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.17         | Ensure system-wide shared library directories must be owned by root                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.18         | Ensure the system-wide shared library directories are group-owned by root or a system account                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.19         | Ensure world-writable directories owner is configured                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.20         | Ensure world-writable directories group-owner is configured                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.21         | Ensure local initialization files do not execute world-writable programs                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.22         | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are mode 0755 or more restrictive | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.23         | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are owned by root                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.24         | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are group-owned by root           | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.25         | Ensure the system-wide shared library files are mode 0755 or more restrictive                                             | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                       | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                       | Yes                      | No                       |
| 7.1.26         | Ensure the system-wide shared library files are owned by root                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.27         | Ensure the system-wide shared library files are group-owned by root                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.2          | Ensure /etc/shadow password fields are not empty                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.3          | Ensure all groups in /etc/passwd exist in /etc/group                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.4          | Ensure shadow group is empty                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.9          | Ensure local interactive user home directories are configured                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.10         | Ensure local interactive user dot files access is configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.11         | Ensure all files and directories in the local interactive user home directory are group-owned by a group that the user is a member of | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.12         | Ensure all files and directories in a local interactive user home directory are mode 0750 or more restrictive                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.13         | Ensure all local initialization files are mode 0740 or more restrictive                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.14         | Ensure local interactive user home directories group-owner is their primary GID                                                       | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: CIS Controls v8 IG 2 Mapped Recommendations

| Recommendation |                                                                                           | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                           | Yes                      | No                       |
| 1.1.1.1        | Ensure cramfs kernel module is not available                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.2        | Ensure freevxfs kernel module is not available                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.3        | Ensure hfs kernel module is not available                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.4        | Ensure hfsplus kernel module is not available                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.5        | Ensure jffs2 kernel module is not available                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.6        | Ensure overlayfs kernel module is not available                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.7        | Ensure squashfs kernel module is not available                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.8        | Ensure udf kernel module is not available                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.9        | Ensure usb-storage kernel module is not available                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.10       | Ensure unused filesystems kernel modules are not available                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.11       | Ensure the operating system disables the ability to load the firewire-core kernel module  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.12       | Ensure a camera is not installed                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.1      | Ensure /tmp is a separate partition                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.2      | Ensure nodev option set on /tmp partition                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.3      | Ensure nosuid option set on /tmp partition                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.4      | Ensure noexec option set on /tmp partition                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.1      | Ensure /dev/shm is a separate partition                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.2      | Ensure nodev option set on /dev/shm partition                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.3      | Ensure nosuid option set on /dev/shm partition                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.4      | Ensure noexec option set on /dev/shm partition                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.1      | Ensure separate partition exists for /home                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.2      | Ensure nodev option set on /home partition                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.3      | Ensure nosuid option set on /home partition                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.5      | Ensure file systems that contain user home directories are mounted with the nosuid option | <input type="checkbox"/> | <input type="checkbox"/> |



| Recommendation |                                                                                             | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                             | Yes                      | No                       |
| 1.1.2.3.6      | Ensure file systems that contain user home directories are mounted with the "noexec" option | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.4.1      | Ensure separate partition exists for /var                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.4.2      | Ensure nodev option set on /var partition                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.4.3      | Ensure nosuid option set on /var partition                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.1      | Ensure separate partition exists for /var/tmp                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.2      | Ensure nodev option set on /var/tmp partition                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.3      | Ensure nosuid option set on /var/tmp partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.4      | Ensure noexec option set on /var/tmp partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.1      | Ensure separate partition exists for /var/log                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.2      | Ensure nodev option set on /var/log partition                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.3      | Ensure nosuid option set on /var/log partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.4      | Ensure noexec option set on /var/log partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.1      | Ensure separate partition exists for /var/log/audit                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.2      | Ensure nodev option set on /var/log/audit partition                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.3      | Ensure nosuid option set on /var/log/audit partition                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.4      | Ensure noexec option set on /var/log/audit partition                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.8.1      | Ensure the "/boot" directory is mounted with the "nosuid" option                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.9.1      | Ensure the "/boot/efi" directory is mounted with the "nosuid" option                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.10.1     | Ensure file systems that are being NFS-imported are mounted with the "nodev" option         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.10.2     | Ensure file systems being imported via NFS are mounted with the "nosuid" option             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.10.3     | Ensure file systems being imported via NFS are mounted with the "noexec" option             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.11.1     | Ensure nodev option set on removable media partitions                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.11.2     | Ensure nosuid option set on removable media partitions                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.11.3     | Ensure noexec option set on removable media partitions                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.12       | Ensure all non-root local partitions are mounted with the "nodev" option                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.3.1        | Ensure all information at rest is encrypted                                                 | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                      | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                      | Yes                      | No                       |
| 1.2.1.1        | Ensure GPG keys are configured                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.2        | Ensure gpgcheck is globally activated                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.3        | Ensure repo_gpgcheck is globally activated                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.4        | Ensure package manager repositories are configured                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.5        | Ensure DNF is configured to perform a signature check on local packages              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2.1        | Ensure updates, patches, and additional security software are installed              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2.2        | Ensure vendor packaged system security patches and updates are installed             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.1        | Ensure SELinux is installed                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.2        | Ensure SELinux is not disabled in bootloader configuration                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.3        | Ensure SELinux policy is configured                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.4        | Ensure the SELinux mode is not disabled                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.5        | Ensure the SELinux mode is enforcing                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.6        | Ensure no unconfined services exist                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.7        | Ensure the MCS Translation Service (mcstrans) is not installed                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.8        | Ensure the operating system has the polycoreutils package installed                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.9        | Ensure SETroubleshoot is not installed                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.10       | Ensure SELinux prevents nonprivileged users from executing privileged functions      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.11       | Ensure SELinux targeted policy is configured                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.1          | Ensure bootloader password is set                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.2          | Ensure access to bootloader config is configured                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.3          | Ensure the operating system requires authentication for rescue mode                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.4          | Ensure the operating system requires authentication upon booting into emergency mode | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.5          | Ensure a unique name is set as the superusers account (BIOS)                         | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                     | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                     | Yes                      | No                       |
| 1.4.6          | Ensure a unique name is set as the superusers account (UEFI)                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1          | Ensure address space layout randomization is enabled                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.2          | Ensure ptrace_scope is restricted                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.8          | Ensure the operating system enables hardening for the BPF JIT                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.10         | Ensure the NX (no-execution) bit flag is set on the system                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.11         | Ensure the operating system disables the use of user namespaces                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.13         | Ensure the operating system is configured to enable DAC on symlinks                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.15         | Ensure the operating system is configured to enable DAC on hardlinks                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.16         | Ensure the operating system restricts exposed kernel pointer addresses access                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.17         | Ensure the operating system is configured to restrict access to the kernel message buffer                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.19         | Ensure the operating system is configured to prevent kernel profiling by unprivileged users                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.20         | Ensure the operating system restricts usage of ptrace to descendant processes                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.21         | Ensure the operating system prevents privilege escalation through the kernel by disabling access to the bpf syscall | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.23         | Ensure the operating system implements the Endpoint Security for Linux Threat Prevention tool                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.1          | Ensure system wide crypto policy is not set to legacy                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.2          | Ensure system wide crypto policy is not set in sshd configuration                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.3          | Ensure system wide crypto policy disables sha1 hash and signature support                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.4          | Ensure system wide crypto policy disables macs less than 128 bits                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.5          | Ensure system wide crypto policy disables cbc for ssh                                                               | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                            | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                            | Yes                      | No                       |
| 1.6.6          | Ensure system wide crypto policy disables chacha20-poly1305 for ssh                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.7          | Ensure system wide crypto policy disables EtM for ssh                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.8          | Ensure system-wide crypto policy is FIPS                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.10         | Ensure system-wide crypto policies are in effect                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.12         | Ensure the OpenSSL library is configured to use only ciphers employing FIPS 140-2-approved algorithms                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.13         | Ensure the OpenSSL library is configured to use only DoD-approved TLS encryption                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.14         | Ensure the GnuTLS library is configured to only allow DoD-approved SSL/TLS Versions                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.4          | Ensure access to /etc/motd is configured                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.5          | Ensure access to /etc/issue is configured                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.6          | Ensure access to /etc/issue.net is configured                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.1          | Ensure GNOME Display Manager is removed                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.4          | Ensure GDM screen locks when the user is idle                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.5          | Ensure GDM screen locks cannot be overridden                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.6          | Ensure GDM automatic mounting of removable media is disabled                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.7          | Ensure GDM disabling automatic mounting of removable media is not overridden                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.8          | Ensure the operating system does not allow an unattended or automatic logon to the system via a graphical user interface   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.9          | Ensure GDM autorun-never is enabled                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.11         | Ensure GDM autorun-never is not overridden                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.12         | Ensure the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.13         | Ensure XDMCP is not enabled                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.14         | Ensure the operating system disables the user logon list for graphical user interfaces                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.16         | Ensure the operating system prevents users from overriding the session idle-delay setting for the graphical user interface | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                  | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                  | Yes                      | No                       |
| 1.8.17         | Ensure the operating system prevents users from overriding the screensaver lock-enabled setting for the graphical user interface | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.18         | Ensure the operating system initiates a session lock for all connection types using smartcard when the smartcard is removed      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.19         | Ensure the operating system enables a user's session lock until that user re-establishes access                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.9            | Ensure the "tmux" package installed                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.13           | Ensure the operating system has the packages required for multifactor authentication                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.1          | Ensure autofs services are not in use                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.2          | Ensure avahi daemon services are not in use                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.3          | Ensure dhcp server services are not in use                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4          | Ensure dns server services are not in use                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.5          | Ensure dnsmasq services are not in use                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.6          | Ensure ftp server services are not in use                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.7          | Ensure message access server services are not in use                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.8          | Ensure network file system services are not in use                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.9          | Ensure nis server services are not in use                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.10         | Ensure print server services are not in use                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.11         | Ensure rpcbind services are not in use                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.12         | Ensure rsync services are not in use                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.13         | Ensure samba file server services are not in use                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.14         | Ensure snmp services are not in use                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.15         | Ensure telnet server services are not in use                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.16         | Ensure tftp server services are not in use                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.17         | Ensure web proxy server services are not in use                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.18         | Ensure web server services are not in use                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.19         | Ensure xinetd services are not in use                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.20         | Ensure X window server services are not in use                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.21         | Ensure only approved services are listening on a network interface                                                               | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                 | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                 | Yes                      | No                       |
| 2.1.22         | Ensure automated bug reporting tools are not installed                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.23         | Ensure mail transfer agents are configured for local-only mode                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.24         | Ensure the sendmail package is not installed                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.25         | Ensure the rsh-server package is not installed                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.26         | Ensure system daemons are prevented from using Kerberos for authentication                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.27         | Ensure the operating system is configured to mask the debug-shell systemd service                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.28         | Ensure the gssproxy package has not been installed on the system                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.29         | Ensure the iprutils package has not been installed on the system                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.30         | Ensure the krb5-server package has not been installed on the system                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.31         | Ensure a TFTP server has not been installed on the system                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.32         | Ensure the tuned package has not been installed on the system                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.34         | Ensure the operating system is configured to prevent unrestricted mail relaying                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.1          | Ensure ftp client is not installed                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.2          | Ensure ldap client is not installed                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.3          | Ensure nis client is not installed                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.4          | Ensure telnet client is not installed                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.5          | Ensure tftp client is not installed                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.6          | Ensure krb5-workstation is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.1          | Ensure time synchronization is in use                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.2          | Ensure chrony is configured                                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.4          | Ensure the operating system is securely comparing internal information system clocks at least every 24 hours with an NTP server | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.5          | Ensure the operating system disables network management of the chrony daemon                                                    | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                | Yes                      | No                       |
| 2.3.6          | Ensure the operating system disables the chrony daemon from acting as a server | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.2        | Ensure permissions on /etc/crontab are configured                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.3        | Ensure permissions on /etc/cron.hourly are configured                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.4        | Ensure permissions on /etc/cron.daily are configured                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.5        | Ensure permissions on /etc/cron.weekly are configured                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.6        | Ensure permissions on /etc/cron.monthly are configured                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.7        | Ensure permissions on /etc/cron.d are configured                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.8        | Ensure crontab is restricted to authorized users                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.2.1        | Ensure at is restricted to authorized users                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5.1          | Ensure USBGuard is installed on the operating system                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5.3          | Ensure the operating system enables Linux audit logging of the USBGuard daemon | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.6.2          | Ensure fapolicyd employs a deny-all, permit-by-exception policy                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.6.3          | Ensure fapolicyd is enabled and running                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1.1          | Ensure IPv6 status is identified                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1.2          | Ensure wireless interfaces are disabled                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1.3          | Ensure bluetooth services are not in use                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1.4          | Ensure network interfaces are not in promiscuous mode                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.1          | Ensure dccp kernel module is not available                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.2          | Ensure tipc kernel module is not available                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.3          | Ensure rds kernel module is not available                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.4          | Ensure sctp kernel module is not available                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.5          | Ensure atm kernel module is not available                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.6          | Ensure bluetooth kernel module is not available                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.7          | Ensure can kernel module is not available                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.1          | Ensure ip forwarding is disabled                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.2          | Ensure packet redirect sending is disabled                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.3          | Ensure bogus icmp responses are ignored                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.4          | Ensure broadcast icmp requests are ignored                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.5          | Ensure icmp redirects are not accepted                                         | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                            | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                            | Yes                      | No                       |
| 3.3.6          | Ensure secure icmp redirects are not accepted                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.7          | Ensure reverse path filtering is enabled                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.8          | Ensure source routed packets are not accepted                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.9          | Ensure suspicious packets are logged                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.10         | Ensure tcp syn cookies is enabled                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.11         | Ensure ipv6 router advertisements are not accepted                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.12         | Ensure net.ipv4.conf.all.forwarding is disabled                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.1        | Ensure nftables base chains exist                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.2        | Ensure host based firewall loopback traffic is configured                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.3        | Ensure firewalld drops unnecessary services and ports                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.4        | Ensure nftables established connections are configured                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.5        | Ensure nftables default deny firewall policy                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2          | Ensure the firewall is configured to remove unnecessary use of functions, ports, protocols, and/or services                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.3          | Ensure firewalld service is enabled and running                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.4          | Ensure nftables is installed                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.5          | Ensure a single firewall configuration utility is in use                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.6          | Ensure "nftables" is configured to allow rate limits on any connection to the system                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.7          | Ensure "firewalld" is installed                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.8          | Ensure "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1          | Ensure openssh-server is installed                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2          | Ensure permissions on /etc/ssh/sshd_config are configured                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3          | Ensure permissions on SSH private host key files are configured                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.4          | Ensure permissions on SSH public host key files are configured                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.5          | Ensure sshd access is configured                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.7          | Ensure sshd Ciphers are configured                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.9          | Ensure sshd DisableForwarding is enabled                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |



| Recommendation |                                                                                                  | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                  | Yes                      | No                       |
| 5.1.10         | Ensure sshd GSSAPIAuthentication is disabled                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.12         | Ensure sshd IgnoreRhosts is enabled                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.13         | Ensure sshd KexAlgorithms is configured                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.15         | Ensure sshd LogLevel is configured                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.16         | Ensure sshd MACs are configured                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.17         | Ensure sshd MaxAuthTries is configured                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.20         | Ensure sshd PermitEmptyPasswords is disabled                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.21         | Ensure sshd PermitRootLogin is disabled                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.23         | Ensure sshd UsePAM is enabled                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.24         | Ensure sshd private key files have a passcode                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.25         | Ensure sshd X11Forwarding is disabled                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.26         | Ensure sshd ClientAliveInterval is configured                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.27         | Ensure sshd ClientAliveCountMax is configured                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.28         | Ensure the SSH server is configured to use only MACs employing FIPS 140-2-approved algorithms    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.29         | Ensure the SSH server is configured to use only ciphers employing FIPS 140-2-approved algorithms | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.30         | Ensure sshd is configured to use only FIPS-validated key exchange algorithms                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.31         | Ensure the SSH server uses strong entropy                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.34         | Ensure sshd IgnoreUserKnownHosts is enabled                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.36         | Ensure sshd KerberosAuthentication is disabled                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.37         | Ensure sshd RekeyLimit is configured                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.39         | Ensure SSH is loaded and active                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1          | Ensure sudo is installed                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2          | Ensure the sudoers file has the default include directory                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3          | Ensure sudo commands use pty                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4          | Ensure sudo log file exists                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.5          | Ensure users must provide password for escalation                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.6          | Ensure the sudoers file restricts sudo access to authorized personnel                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.7          | Ensure re-authentication for privilege escalation is not disabled globally                       | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                               | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                               | Yes                      | No                       |
| 5.2.8          | Ensure the sudoers security policy is configured to use the invoking user's password for privilege escalation | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.9          | Ensure sudo timestamp_timeout is configured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.10         | Ensure access to the su command is restricted                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.11         | Ensure pam_succeed_if does not exist in /etc/pam.d/sudo                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.1        | Ensure active authselect profile includes pam modules                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.2        | Ensure pam_faillock module is enabled                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.3        | Ensure pam_pwquality module is enabled                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.4        | Ensure pam_pwhistory module is enabled                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.1      | Ensure password failed attempts lockout is configured                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.2      | Ensure password unlock time is configured                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.3      | Ensure password failed attempts lockout includes root account                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.4      | Ensure deny is configured on the pam_faillock module                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.5      | Ensure deny is configured in /etc/security/faillock.conf                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.6      | Ensure fail_interval is configured on the pam_faillock module                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.7      | Ensure fail_interval is configured in /etc/security/faillock.conf                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.8      | Ensure unlock_time is configured on the pam_faillock module                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.9      | Ensure unlock_time is configured in /etc/security/faillock.conf                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.10     | Ensure dir is configured on the pam_faillock module                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.11     | Ensure dir is configured in /etc/security/faillock.conf                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.14     | Ensure audit is set on the pam_faillock module                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.15     | Ensure audit is set in /etc/security/faillock.conf                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.16     | Ensure even_deny_root is set on the pam_faillock module                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.17     | Ensure even_deny_root is set in /etc/security/faillock.conf                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.18     | Ensure the use of a non-default faillock tally directory while SELinux enforces a targeted policy             | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                              | Set Correctly            |                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                              | Yes                      | No                       |
| 5.3.3.1.19     | Ensure the use of a non-default faillock tally directory on the pam_faillock module while SELinux enforces a targeted policy | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.1      | Ensure password number of changed characters is configured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.2      | Ensure password length is configured                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.3      | Ensure password complexity is configured                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.4      | Ensure password same consecutive characters is configured                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.5      | Ensure password maximum sequential characters is configured                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.6      | Ensure password dictionary check is enabled                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.7      | Ensure password quality is enforced for the root user                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.8      | Ensure the operating system enforces a minimum 15-character password length                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.9      | Ensure ucredit is configured in /etc/security/pwquality.conf                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.10     | Ensure lcredit is configured in /etc/security/pwquality.conf                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.11     | Ensure dcredit is configured in /etc/security/pwquality.conf                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.12     | Ensure ocredit is configured in /etc/security/pwquality.conf                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.13     | Ensure maxclassrepeat is configured in /etc/security/pwquality.conf                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.14     | Ensure minclass is configured in /etc/security/pwquality.conf                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.15     | Ensure difok is configured in /etc/security/pwquality.conf                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.16     | Ensure dictcheck is configured                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.17     | Ensure retry is configured on the pam_pwquality module in /etc/pam.d/system-auth                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.18     | Ensure retry is configured on the pam_pwquality module in /etc/pam.d/password-auth                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.19     | Ensure retry is configured in /etc/security/pwquality.conf                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.1      | Ensure password history remember is configured                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.2      | Ensure password history is enforced for the root user                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                  | Set Correctly            |                          |
|----------------|------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                  | Yes                      | No                       |
| 5.3.3.3.3      | Ensure pam_pwhistory includes use_authok                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.4      | Ensure remember is configured on the pam_pwhistory module in /etc/pam.d/password-auth                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.5      | Ensure remember is configured on the pam_pwhistory module in /etc/pam.d/system-auth                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.1      | Ensure pam_unix does not include nullok                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.2      | Ensure pam_unix does not include remember                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.3      | Ensure pam_unix includes a strong password hashing algorithm                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.4      | Ensure pam_unix includes use_authok                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.5      | Ensure pam_unix includes a FIPS 140-2 approved hashing algorithm                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.6.1      | Ensure the operating system uses multifactor authentication for local access to accounts                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.6.3      | Ensure the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.1        | Ensure password expiration is configured                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.2        | Ensure minimum password days is configured                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.3        | Ensure password expiration warning days is configured                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.4        | Ensure strong password hashing algorithm is configured                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.5        | Ensure inactive password lock is configured                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.6        | Ensure all users last password change date is in the past                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.7        | Ensure passwords use FIPS 140-2 approved cryptographic hashing algorithm                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.8        | Ensure minimum number of hashing rounds is configured                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.9        | Ensure existing passwords use FIPS 140-2 approved cryptographic hashing algorithm                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.12       | Ensure pass_min_len is configured                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.13       | Ensure the maximum time period for existing passwords is restricted to 60 days                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.2        | Ensure root is the only GID 0 account                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.3        | Ensure group root is the only GID 0 group                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.4        | Ensure root account access is controlled                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.6        | Ensure root user umask is configured                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                                          | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                          | Yes                      | No                       |
| 5.4.2.7        | Ensure system accounts do not have a valid login shell                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.8        | Ensure accounts without a valid login shell are locked                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.2        | Ensure default user shell timeout is configured                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.3        | Ensure default user umask is configured                                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.5        | Ensure the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.6        | Ensure the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.7        | Ensure the operating system enforces a 60-day maximum password lifetime for new user accounts                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.8        | Ensure the umask default for installed shells is "077"                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.9        | Ensure the default umask for all local interactive users is "077"                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.10       | Ensure the operating system initiates a session lock after 15 minutes of inactivity                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.11       | Ensure the operating system prevents users from disabling the tmux terminal multiplexer                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.12       | Ensure the operating system's shell initialization file is configured to start each shell with the tmux terminal multiplexer                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.13       | Ensure the operating system enables the user to initiate a session lock                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.16       | Ensure StopIdleSessionSec is configured                                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.1      | Ensure journald service is enabled and active                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.2      | Ensure journald log file access is configured                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.3      | Ensure journald log file rotation is configured                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.4      | Ensure journald ForwardToSyslog is disabled                                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.5      | Ensure journald Storage is configured                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.6      | Ensure journald Compress is configured                                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.1      | Ensure systemd-journal-remote is installed                                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.2      | Ensure systemd-journal-remote authentication is configured                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.3      | Ensure systemd-journal-upload is enabled and active                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                              | Set Correctly            |                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                              | Yes                      | No                       |
| 6.2.1.2.4      | Ensure systemd-journal-remote service is not in use                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.1        | Ensure rsyslog is installed                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.2        | Ensure rsyslog service is enabled and active                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.3        | Ensure all remote access methods are monitored                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.4        | Ensure journald is configured to send logs to rsyslog                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.5        | Ensure rsyslog log file creation mode is configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.6        | Ensure rsyslog logging is configured                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.7        | Ensure rsyslog is configured to send logs to a remote log host                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.8        | Ensure rsyslog is not configured to receive logs from a remote client                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.9        | Ensure logrotate is configured                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.10       | Ensure rsyslog is configured to log cron events                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.11       | Ensure the rsyslog service is enabled and active                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.12       | Ensure the operating system has the packages required for encrypting offloaded audit logs                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.13       | Ensure the the operating system authenticates the remote logging server for off-loading audit logs                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.14       | Ensure the operating system encrypts audit records off-loaded onto a different system or media from the system being audited | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.15       | Ensure the audit system off-loads audit records onto a different system or media from the system being audited               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.1        | Ensure access to all logfiles has been configured                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.2        | Ensure /var/log/messages mode is configured                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.3        | Ensure /var/log/messages owner is configured                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.4        | Ensure /var/log/messages group owner is configured                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.5        | Ensure /var/log is mode is configured                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.6        | Ensure /var/log owner is configured                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.7        | Ensure /var/log group owner is configured                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.8        | Ensure administrators are notified if an audit processing failure occurs by modifying /etc/aliases                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.1        | Ensure auditd packages are installed                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                                                | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                                | Yes                      | No                       |
| 6.3.1.2        | Ensure auditing for processes that start prior to auditd is enabled                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.3        | Ensure audit_backlog_limit is sufficient                                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.4        | Ensure auditd service is enabled and active                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.5        | Ensure the operating system allocates a sufficient audit_backlog_limit to capture processes that start prior to the audit daemon                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.6        | Ensure the operating system's audit daemon is configured to include local events                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.7        | Ensure the operating system's audit daemon is configured to label all off-loaded audit logs                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.8        | Ensure the operating system's audit daemon is configured to resolve audit information before writing to disk                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.1        | Ensure audit log storage size is configured                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.2        | Ensure audit logs are not automatically deleted                                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.3        | Ensure system is disabled when audit logs are full                                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.4        | Ensure system warns when audit logs are low on space                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.5        | Ensure the operating system allocates audit record storage capacity                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.6        | Ensure the SA and ISSO are notified in the event of an audit processing failure                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.7        | Ensure the operating system notifies the SA and ISSO when allocated audit record storage volume reaches 75 percent                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.8        | Ensure the operating system takes action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.9        | Ensure the audit system is configured to take an appropriate action when the internal event queue is full                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.1        | Ensure changes to system administration scope (sudoers) is collected                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.2        | Ensure actions as another user are always logged                                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.3        | Ensure events that modify the sudo log file are collected                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                      | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                      | Yes                      | No                       |
| 6.3.3.4        | Ensure events that modify date and time information are collected                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.5        | Ensure events that modify the system's network environment are collected             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.6        | Ensure use of privileged commands are collected                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.7        | Ensure unsuccessful file access attempts are collected                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.8        | Ensure events that modify user/group information are collected                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.9        | Ensure discretionary access control permission modification events are collected     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.10       | Ensure successful file system mounts are collected                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.11       | Ensure session initiation information is collected                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.12       | Ensure login and logout events are collected                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.13       | Ensure file deletion events by users are collected                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.14       | Ensure events that modify the system's Mandatory Access Controls are collected       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.15       | Ensure successful and unsuccessful attempts to use the chcon command are collected   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.16       | Ensure successful and unsuccessful attempts to use the setfacl command are collected | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.17       | Ensure successful and unsuccessful attempts to use the chacl command are collected   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.18       | Ensure successful and unsuccessful attempts to use the usermod command are collected | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.19       | Ensure kernel module loading unloading and modification is collected                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.20       | Ensure the audit configuration is immutable                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.21       | Ensure the running and on disk configuration is the same                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.22       | Ensure successful and unsuccessful attempts to use the su command are collected      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.23       | Ensure successful and unsuccessful attempts to use the sudo command are collected    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.24       | Ensure successful and unsuccessful attempts to use the chsh command are collected    | <input type="checkbox"/> | <input type="checkbox"/> |



| Recommendation |                                                                                                  | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                  | Yes                      | No                       |
| 6.3.3.25       | Ensure successful and unsuccessful attempts to use the crontab command are collected             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.26       | Ensure successful and unsuccessful attempts to use the gpasswd command are collected             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.27       | Ensure successful and unsuccessful attempts to use the newgrp command are collected              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.28       | Ensure successful and unsuccessful attempts to use the pam_timestamp_check command are collected | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.29       | Ensure successful and unsuccessful attempts to use the ssh-keysign command are collected         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.30       | Ensure successful and unsuccessful attempts to use the unix_chkpwd command are collected         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.31       | Ensure successful and unsuccessful attempts to use the setsebool command are collected           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.32       | Ensure successful and unsuccessful attempts to use the userhelper command are collected          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.33       | Ensure successful and unsuccessful attempts to use the setfiles command are collected            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.34       | Ensure successful and unsuccessful attempts to use the semanage command are collected            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.35       | Ensure successful and unsuccessful attempts to use the postqueue command are collected           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.36       | Ensure successful and unsuccessful attempts to use the postdrop command are collected            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.37       | Ensure successful and unsuccessful attempts to use the unix_update command are collected         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.38       | Ensure successful and unsuccessful attempts to use the umount command are collected              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.39       | Ensure successful and unsuccessful attempts to use the mount command are collected               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.40       | Ensure successful and unsuccessful attempts to use the ssh-agent command are collected           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.41       | Ensure successful and unsuccessful attempts to use the passwd command are collected              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.42       | Ensure successful and unsuccessful attempts to use the chage command are collected               | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                     | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                     | Yes                      | No                       |
| 6.3.3.43       | Ensure the audit system prevents unauthorized changes to logon UIDs                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.44       | Ensure successful and unsuccessful modifications to the faillock file are collected | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.1        | Ensure the audit log file directory mode is configured                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.2        | Ensure audit log files mode is configured                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.3        | Ensure audit log files owner is configured                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.4        | Ensure audit log files group owner is configured                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.5        | Ensure audit configuration files mode is configured                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.6        | Ensure audit configuration files owner is configured                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.7        | Ensure audit configuration files group owner is configured                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.8        | Ensure audit tools mode is configured                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.9        | Ensure audit tools owner is configured                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.10       | Ensure audit tools group owner is configured                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.11       | Ensure the audit logs are group-owned by root                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.12       | Ensure audit tools are mode 0755 or more restrictive                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.13       | Ensure the audit tools are owned by root                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.14       | Ensure audit tools are group owned by root                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.15       | Ensure the audit log file directories are mode 0700 or more restrictive             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.16       | Ensure the audit log file directory is owned by root                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.17       | Ensure audit log files group owner is root                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.18       | Ensure audit log files are mode 0600 or more restrictive                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.1          | Ensure permissions on /etc/passwd are configured                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.2          | Ensure permissions on /etc/passwd- are configured                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.3          | Ensure permissions on /etc/group are configured                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.4          | Ensure permissions on /etc/group- are configured                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.5          | Ensure permissions on /etc/shadow are configured                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.6          | Ensure permissions on /etc/shadow- are configured                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.7          | Ensure permissions on /etc/gshadow are configured                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.8          | Ensure permissions on /etc/gshadow- are configured                                  | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                           | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                           | Yes                      | No                       |
| 7.1.9          | Ensure permissions on /etc/shells are configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.10         | Ensure permissions on /etc/security/opasswd are configured                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.11         | Ensure world writable files and directories are secured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.12         | Ensure no files or directories without an owner and a group exist                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.13         | Ensure SUID and SGID files are reviewed                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.14         | Ensure there are no ".shosts" files on the operating system                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.15         | Ensure there are no "shosts.equiv" files on the operating system                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.16         | Ensure system-wide shared library directories have mode 755 or less permissive                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.17         | Ensure system-wide shared library directories must be owned by root                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.18         | Ensure the system-wide shared library directories are group-owned by root or a system account                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.19         | Ensure world-writable directories owner is configured                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.20         | Ensure world-writable directories group-owner is configured                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.21         | Ensure local initialization files do not execute world-writable programs                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.22         | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are mode 0755 or more restrictive | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.23         | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are owned by root                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.24         | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are group-owned by root           | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.25         | Ensure the system-wide shared library files are mode 0755 or more restrictive                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.26         | Ensure the system-wide shared library files are owned by root                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.27         | Ensure the system-wide shared library files are group-owned by root                                                       | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                       | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                       | Yes                      | No                       |
| 7.2.1          | Ensure accounts in /etc/passwd use shadowed passwords                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.2          | Ensure /etc/shadow password fields are not empty                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.3          | Ensure all groups in /etc/passwd exist in /etc/group                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.4          | Ensure shadow group is empty                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.9          | Ensure local interactive user home directories are configured                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.10         | Ensure local interactive user dot files access is configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.11         | Ensure all files and directories in the local interactive user home directory are group-owned by a group that the user is a member of | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.12         | Ensure all files and directories in a local interactive user home directory are mode 0750 or more restrictive                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.13         | Ensure all local initialization files are mode 0740 or more restrictive                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.14         | Ensure local interactive user home directories group-owner is their primary GID                                                       | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: CIS Controls v8 IG 3 Mapped Recommendations

| Recommendation |                                                                                           | Set Correctly            |                          |
|----------------|-------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                           | Yes                      | No                       |
| 1.1.1.1        | Ensure cramfs kernel module is not available                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.2        | Ensure freevxfs kernel module is not available                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.3        | Ensure hfs kernel module is not available                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.4        | Ensure hfsplus kernel module is not available                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.5        | Ensure jffs2 kernel module is not available                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.6        | Ensure overlayfs kernel module is not available                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.7        | Ensure squashfs kernel module is not available                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.8        | Ensure udf kernel module is not available                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.9        | Ensure usb-storage kernel module is not available                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.10       | Ensure unused filesystems kernel modules are not available                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.11       | Ensure the operating system disables the ability to load the firewire-core kernel module  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.1.12       | Ensure a camera is not installed                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.1      | Ensure /tmp is a separate partition                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.2      | Ensure nodev option set on /tmp partition                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.3      | Ensure nosuid option set on /tmp partition                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.1.4      | Ensure noexec option set on /tmp partition                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.1      | Ensure /dev/shm is a separate partition                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.2      | Ensure nodev option set on /dev/shm partition                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.3      | Ensure nosuid option set on /dev/shm partition                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.2.4      | Ensure noexec option set on /dev/shm partition                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.1      | Ensure separate partition exists for /home                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.2      | Ensure nodev option set on /home partition                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.3      | Ensure nosuid option set on /home partition                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.3.5      | Ensure file systems that contain user home directories are mounted with the nosuid option | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                             | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                             | Yes                      | No                       |
| 1.1.2.3.6      | Ensure file systems that contain user home directories are mounted with the "noexec" option | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.4.1      | Ensure separate partition exists for /var                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.4.2      | Ensure nodev option set on /var partition                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.4.3      | Ensure nosuid option set on /var partition                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.1      | Ensure separate partition exists for /var/tmp                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.2      | Ensure nodev option set on /var/tmp partition                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.3      | Ensure nosuid option set on /var/tmp partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.5.4      | Ensure noexec option set on /var/tmp partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.1      | Ensure separate partition exists for /var/log                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.2      | Ensure nodev option set on /var/log partition                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.3      | Ensure nosuid option set on /var/log partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.6.4      | Ensure noexec option set on /var/log partition                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.1      | Ensure separate partition exists for /var/log/audit                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.2      | Ensure nodev option set on /var/log/audit partition                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.3      | Ensure nosuid option set on /var/log/audit partition                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.7.4      | Ensure noexec option set on /var/log/audit partition                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.8.1      | Ensure the "/boot" directory is mounted with the "nosuid" option                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.9.1      | Ensure the "/boot/efi" directory is mounted with the "nosuid" option                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.10.1     | Ensure file systems that are being NFS-imported are mounted with the "nodev" option         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.10.2     | Ensure file systems being imported via NFS are mounted with the "nosuid" option             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.10.3     | Ensure file systems being imported via NFS are mounted with the "noexec" option             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.11.1     | Ensure nodev option set on removable media partitions                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.11.2     | Ensure nosuid option set on removable media partitions                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.11.3     | Ensure noexec option set on removable media partitions                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2.12       | Ensure all non-root local partitions are mounted with the "nodev" option                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.3.1        | Ensure all information at rest is encrypted                                                 | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                      | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                      | Yes                      | No                       |
| 1.2.1.1        | Ensure GPG keys are configured                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.2        | Ensure gpgcheck is globally activated                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.3        | Ensure repo_gpgcheck is globally activated                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.4        | Ensure package manager repositories are configured                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1.5        | Ensure DNF is configured to perform a signature check on local packages              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2.1        | Ensure updates, patches, and additional security software are installed              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2.2        | Ensure vendor packaged system security patches and updates are installed             | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.1        | Ensure SELinux is installed                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.2        | Ensure SELinux is not disabled in bootloader configuration                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.3        | Ensure SELinux policy is configured                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.4        | Ensure the SELinux mode is not disabled                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.5        | Ensure the SELinux mode is enforcing                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.6        | Ensure no unconfined services exist                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.7        | Ensure the MCS Translation Service (mcstrans) is not installed                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.8        | Ensure the operating system has the polycoreutils package installed                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.9        | Ensure SETroubleshoot is not installed                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.10       | Ensure SELinux prevents nonprivileged users from executing privileged functions      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.3.1.11       | Ensure SELinux targeted policy is configured                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.1          | Ensure bootloader password is set                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.2          | Ensure access to bootloader config is configured                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.3          | Ensure the operating system requires authentication for rescue mode                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.4          | Ensure the operating system requires authentication upon booting into emergency mode | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.4.5          | Ensure a unique name is set as the superusers account (BIOS)                         | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                     | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                     | Yes                      | No                       |
| 1.4.6          | Ensure a unique name is set as the superusers account (UEFI)                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.1          | Ensure address space layout randomization is enabled                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.2          | Ensure ptrace_scope is restricted                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.8          | Ensure the operating system enables hardening for the BPF JIT                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.10         | Ensure the NX (no-execution) bit flag is set on the system                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.11         | Ensure the operating system disables the use of user namespaces                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.13         | Ensure the operating system is configured to enable DAC on symlinks                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.15         | Ensure the operating system is configured to enable DAC on hardlinks                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.16         | Ensure the operating system restricts exposed kernel pointer addresses access                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.17         | Ensure the operating system is configured to restrict access to the kernel message buffer                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.19         | Ensure the operating system is configured to prevent kernel profiling by unprivileged users                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.20         | Ensure the operating system restricts usage of ptrace to descendant processes                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.21         | Ensure the operating system prevents privilege escalation through the kernel by disabling access to the bpf syscall | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.5.23         | Ensure the operating system implements the Endpoint Security for Linux Threat Prevention tool                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.1          | Ensure system wide crypto policy is not set to legacy                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.2          | Ensure system wide crypto policy is not set in sshd configuration                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.3          | Ensure system wide crypto policy disables sha1 hash and signature support                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.4          | Ensure system wide crypto policy disables macs less than 128 bits                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.5          | Ensure system wide crypto policy disables cbc for ssh                                                               | <input type="checkbox"/> | <input type="checkbox"/> |



| Recommendation |                                                                                                                            | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                            | Yes                      | No                       |
| 1.6.6          | Ensure system wide crypto policy disables chacha20-poly1305 for ssh                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.7          | Ensure system wide crypto policy disables EtM for ssh                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.8          | Ensure system-wide crypto policy is FIPS                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.10         | Ensure system-wide crypto policies are in effect                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.12         | Ensure the OpenSSL library is configured to use only ciphers employing FIPS 140-2-approved algorithms                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.13         | Ensure the OpenSSL library is configured to use only DoD-approved TLS encryption                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.6.14         | Ensure the GnuTLS library is configured to only allow DoD-approved SSL/TLS Versions                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.4          | Ensure access to /etc/motd is configured                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.5          | Ensure access to /etc/issue is configured                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.6          | Ensure access to /etc/issue.net is configured                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.1          | Ensure GNOME Display Manager is removed                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.4          | Ensure GDM screen locks when the user is idle                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.5          | Ensure GDM screen locks cannot be overridden                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.6          | Ensure GDM automatic mounting of removable media is disabled                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.7          | Ensure GDM disabling automatic mounting of removable media is not overridden                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.8          | Ensure the operating system does not allow an unattended or automatic logon to the system via a graphical user interface   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.9          | Ensure GDM autorun-never is enabled                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.11         | Ensure GDM autorun-never is not overridden                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.12         | Ensure the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.13         | Ensure XDMCP is not enabled                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.14         | Ensure the operating system disables the user logon list for graphical user interfaces                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.16         | Ensure the operating system prevents users from overriding the session idle-delay setting for the graphical user interface | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                  | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                  | Yes                      | No                       |
| 1.8.17         | Ensure the operating system prevents users from overriding the screensaver lock-enabled setting for the graphical user interface | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.18         | Ensure the operating system initiates a session lock for all connection types using smartcard when the smartcard is removed      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.19         | Ensure the operating system enables a user's session lock until that user re-establishes access                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.9            | Ensure the "tmux" package installed                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.13           | Ensure the operating system has the packages required for multifactor authentication                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.1          | Ensure autofs services are not in use                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.2          | Ensure avahi daemon services are not in use                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.3          | Ensure dhcp server services are not in use                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.4          | Ensure dns server services are not in use                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.5          | Ensure dnsmasq services are not in use                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.6          | Ensure ftp server services are not in use                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.7          | Ensure message access server services are not in use                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.8          | Ensure network file system services are not in use                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.9          | Ensure nis server services are not in use                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.10         | Ensure print server services are not in use                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.11         | Ensure rpcbind services are not in use                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.12         | Ensure rsync services are not in use                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.13         | Ensure samba file server services are not in use                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.14         | Ensure snmp services are not in use                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.15         | Ensure telnet server services are not in use                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.16         | Ensure tftp server services are not in use                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.17         | Ensure web proxy server services are not in use                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.18         | Ensure web server services are not in use                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.19         | Ensure xinetd services are not in use                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.20         | Ensure X window server services are not in use                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.21         | Ensure only approved services are listening on a network interface                                                               | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                 | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                 | Yes                      | No                       |
| 2.1.22         | Ensure automated bug reporting tools are not installed                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.23         | Ensure mail transfer agents are configured for local-only mode                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.24         | Ensure the sendmail package is not installed                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.25         | Ensure the rsh-server package is not installed                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.26         | Ensure system daemons are prevented from using Kerberos for authentication                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.27         | Ensure the operating system is configured to mask the debug-shell systemd service                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.28         | Ensure the gssproxy package has not been installed on the system                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.29         | Ensure the iprutils package has not been installed on the system                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.30         | Ensure the krb5-server package has not been installed on the system                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.31         | Ensure a TFTP server has not been installed on the system                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.32         | Ensure the tuned package has not been installed on the system                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1.34         | Ensure the operating system is configured to prevent unrestricted mail relaying                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.1          | Ensure ftp client is not installed                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.2          | Ensure ldap client is not installed                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.3          | Ensure nis client is not installed                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.4          | Ensure telnet client is not installed                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.5          | Ensure tftp client is not installed                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2.6          | Ensure krb5-workstation is not installed                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.1          | Ensure time synchronization is in use                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.2          | Ensure chrony is configured                                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.4          | Ensure the operating system is securely comparing internal information system clocks at least every 24 hours with an NTP server | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.5          | Ensure the operating system disables network management of the chrony daemon                                                    | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                | Yes                      | No                       |
| 2.3.6          | Ensure the operating system disables the chrony daemon from acting as a server | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.2        | Ensure permissions on /etc/crontab are configured                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.3        | Ensure permissions on /etc/cron.hourly are configured                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.4        | Ensure permissions on /etc/cron.daily are configured                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.5        | Ensure permissions on /etc/cron.weekly are configured                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.6        | Ensure permissions on /etc/cron.monthly are configured                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.7        | Ensure permissions on /etc/cron.d are configured                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.8        | Ensure crontab is restricted to authorized users                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.2.1        | Ensure at is restricted to authorized users                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5.1          | Ensure USBGuard is installed on the operating system                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.5.3          | Ensure the operating system enables Linux audit logging of the USBGuard daemon | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.6.2          | Ensure fapolicyd employs a deny-all, permit-by-exception policy                | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.6.3          | Ensure fapolicyd is enabled and running                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1.1          | Ensure IPv6 status is identified                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1.2          | Ensure wireless interfaces are disabled                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1.3          | Ensure bluetooth services are not in use                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.1.4          | Ensure network interfaces are not in promiscuous mode                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.1          | Ensure dccp kernel module is not available                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.2          | Ensure tipc kernel module is not available                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.3          | Ensure rds kernel module is not available                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.4          | Ensure sctp kernel module is not available                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.5          | Ensure atm kernel module is not available                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.6          | Ensure bluetooth kernel module is not available                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2.7          | Ensure can kernel module is not available                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.1          | Ensure ip forwarding is disabled                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.2          | Ensure packet redirect sending is disabled                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.3          | Ensure bogus icmp responses are ignored                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.4          | Ensure broadcast icmp requests are ignored                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.5          | Ensure icmp redirects are not accepted                                         | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                            | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                            | Yes                      | No                       |
| 3.3.6          | Ensure secure icmp redirects are not accepted                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.7          | Ensure reverse path filtering is enabled                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.8          | Ensure source routed packets are not accepted                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.9          | Ensure suspicious packets are logged                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.10         | Ensure tcp syn cookies is enabled                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.11         | Ensure ipv6 router advertisements are not accepted                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3.12         | Ensure net.ipv4.conf.all.forwarding is disabled                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.1        | Ensure nftables base chains exist                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.2        | Ensure host based firewall loopback traffic is configured                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.3        | Ensure firewalld drops unnecessary services and ports                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.4        | Ensure nftables established connections are configured                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.1.5        | Ensure nftables default deny firewall policy                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.2          | Ensure the firewall is configured to remove unnecessary use of functions, ports, protocols, and/or services                | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.3          | Ensure firewalld service is enabled and running                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.4          | Ensure nftables is installed                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.5          | Ensure a single firewall configuration utility is in use                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.6          | Ensure "nftables" is configured to allow rate limits on any connection to the system                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.7          | Ensure "firewalld" is installed                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1.8          | Ensure "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.1          | Ensure openssh-server is installed                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.2          | Ensure permissions on /etc/ssh/sshd_config are configured                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.3          | Ensure permissions on SSH private host key files are configured                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.4          | Ensure permissions on SSH public host key files are configured                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.5          | Ensure sshd access is configured                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.7          | Ensure sshd Ciphers are configured                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.9          | Ensure sshd DisableForwarding is enabled                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                  | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                  | Yes                      | No                       |
| 5.1.10         | Ensure sshd GSSAPIAuthentication is disabled                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.12         | Ensure sshd IgnoreRhosts is enabled                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.13         | Ensure sshd KexAlgorithms is configured                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.15         | Ensure sshd LogLevel is configured                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.16         | Ensure sshd MACs are configured                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.17         | Ensure sshd MaxAuthTries is configured                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.20         | Ensure sshd PermitEmptyPasswords is disabled                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.21         | Ensure sshd PermitRootLogin is disabled                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.23         | Ensure sshd UsePAM is enabled                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.24         | Ensure sshd private key files have a passcode                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.25         | Ensure sshd X11Forwarding is disabled                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.26         | Ensure sshd ClientAliveInterval is configured                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.27         | Ensure sshd ClientAliveCountMax is configured                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.28         | Ensure the SSH server is configured to use only MACs employing FIPS 140-2-approved algorithms    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.29         | Ensure the SSH server is configured to use only ciphers employing FIPS 140-2-approved algorithms | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.30         | Ensure sshd is configured to use only FIPS-validated key exchange algorithms                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.31         | Ensure the SSH server uses strong entropy                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.34         | Ensure sshd IgnoreUserKnownHosts is enabled                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.36         | Ensure sshd KerberosAuthentication is disabled                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.37         | Ensure sshd RekeyLimit is configured                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.39         | Ensure SSH is loaded and active                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.1          | Ensure sudo is installed                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.2          | Ensure the sudoers file has the default include directory                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.3          | Ensure sudo commands use pty                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.4          | Ensure sudo log file exists                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.5          | Ensure users must provide password for escalation                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.6          | Ensure the sudoers file restricts sudo access to authorized personnel                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.7          | Ensure re-authentication for privilege escalation is not disabled globally                       | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                               | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                               | Yes                      | No                       |
| 5.2.8          | Ensure the sudoers security policy is configured to use the invoking user's password for privilege escalation | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.9          | Ensure sudo timestamp_timeout is configured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.10         | Ensure access to the su command is restricted                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2.11         | Ensure pam_succeed_if does not exist in /etc/pam.d/sudo                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.1        | Ensure active authselect profile includes pam modules                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.2        | Ensure pam_faillock module is enabled                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.3        | Ensure pam_pwquality module is enabled                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.4        | Ensure pam_pwhistory module is enabled                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.1      | Ensure password failed attempts lockout is configured                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.2      | Ensure password unlock time is configured                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.3      | Ensure password failed attempts lockout includes root account                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.4      | Ensure deny is configured on the pam_faillock module                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.5      | Ensure deny is configured in /etc/security/faillock.conf                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.6      | Ensure fail_interval is configured on the pam_faillock module                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.7      | Ensure fail_interval is configured in /etc/security/faillock.conf                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.8      | Ensure unlock_time is configured on the pam_faillock module                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.9      | Ensure unlock_time is configured in /etc/security/faillock.conf                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.10     | Ensure dir is configured on the pam_faillock module                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.11     | Ensure dir is configured in /etc/security/faillock.conf                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.14     | Ensure audit is set on the pam_faillock module                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.15     | Ensure audit is set in /etc/security/faillock.conf                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.16     | Ensure even_deny_root is set on the pam_faillock module                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.17     | Ensure even_deny_root is set in /etc/security/faillock.conf                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.1.18     | Ensure the use of a non-default faillock tally directory while SELinux enforces a targeted policy             | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                              | Set Correctly            |                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                              | Yes                      | No                       |
| 5.3.3.1.19     | Ensure the use of a non-default faillock tally directory on the pam_faillock module while SELinux enforces a targeted policy | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.1      | Ensure password number of changed characters is configured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.2      | Ensure password length is configured                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.3      | Ensure password complexity is configured                                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.4      | Ensure password same consecutive characters is configured                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.5      | Ensure password maximum sequential characters is configured                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.6      | Ensure password dictionary check is enabled                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.7      | Ensure password quality is enforced for the root user                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.8      | Ensure the operating system enforces a minimum 15-character password length                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.9      | Ensure ucredit is configured in /etc/security/pwquality.conf                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.10     | Ensure lcredit is configured in /etc/security/pwquality.conf                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.11     | Ensure dcredit is configured in /etc/security/pwquality.conf                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.12     | Ensure ocredit is configured in /etc/security/pwquality.conf                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.13     | Ensure maxclassrepeat is configured in /etc/security/pwquality.conf                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.14     | Ensure minclass is configured in /etc/security/pwquality.conf                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.15     | Ensure difok is configured in /etc/security/pwquality.conf                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.16     | Ensure dictcheck is configured                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.17     | Ensure retry is configured on the pam_pwquality module in /etc/pam.d/system-auth                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.18     | Ensure retry is configured on the pam_pwquality module in /etc/pam.d/password-auth                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.2.19     | Ensure retry is configured in /etc/security/pwquality.conf                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.1      | Ensure password history remember is configured                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.2      | Ensure password history is enforced for the root user                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |



| Recommendation |                                                                                                                  | Set Correctly            |                          |
|----------------|------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                  | Yes                      | No                       |
| 5.3.3.3.3      | Ensure pam_pwhistory includes use_authok                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.4      | Ensure remember is configured on the pam_pwhistory module in /etc/pam.d/password-auth                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.3.5      | Ensure remember is configured on the pam_pwhistory module in /etc/pam.d/system-auth                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.1      | Ensure pam_unix does not include nullok                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.2      | Ensure pam_unix does not include remember                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.3      | Ensure pam_unix includes a strong password hashing algorithm                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.4      | Ensure pam_unix includes use_authok                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.4.5      | Ensure pam_unix includes a FIPS 140-2 approved hashing algorithm                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.6.1      | Ensure the operating system uses multifactor authentication for local access to accounts                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.3.6.3      | Ensure the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.1        | Ensure password expiration is configured                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.2        | Ensure minimum password days is configured                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.3        | Ensure password expiration warning days is configured                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.4        | Ensure strong password hashing algorithm is configured                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.5        | Ensure inactive password lock is configured                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.6        | Ensure all users last password change date is in the past                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.7        | Ensure passwords use FIPS 140-2 approved cryptographic hashing algorithm                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.8        | Ensure minimum number of hashing rounds is configured                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.9        | Ensure existing passwords use FIPS 140-2 approved cryptographic hashing algorithm                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.12       | Ensure pass_min_len is configured                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.1.13       | Ensure the maximum time period for existing passwords is restricted to 60 days                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.2        | Ensure root is the only GID 0 account                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.3        | Ensure group root is the only GID 0 group                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.4        | Ensure root account access is controlled                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.6        | Ensure root user umask is configured                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                                          | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                          | Yes                      | No                       |
| 5.4.2.7        | Ensure system accounts do not have a valid login shell                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.8        | Ensure accounts without a valid login shell are locked                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.2        | Ensure default user shell timeout is configured                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.3        | Ensure default user umask is configured                                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.5        | Ensure the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.6        | Ensure the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.7        | Ensure the operating system enforces a 60-day maximum password lifetime for new user accounts                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.8        | Ensure the umask default for installed shells is "077"                                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.9        | Ensure the default umask for all local interactive users is "077"                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.10       | Ensure the operating system initiates a session lock after 15 minutes of inactivity                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.11       | Ensure the operating system prevents users from disabling the tmux terminal multiplexer                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.12       | Ensure the operating system's shell initialization file is configured to start each shell with the tmux terminal multiplexer                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.13       | Ensure the operating system enables the user to initiate a session lock                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.16       | Ensure StopIdleSessionSec is configured                                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.1          | Ensure AIDE is installed                                                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.2          | Ensure filesystem integrity is regularly checked                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.4          | Ensure AIDE is configured to use cryptographic mechanisms to protect the integrity of audit tools                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.5          | Ensure the file integrity tool is configured to verify ACLs                                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.6          | Ensure the file integrity tool is configured to verify extended attributes                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.1      | Ensure journald service is enabled and active                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.2      | Ensure journald log file access is configured                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.3      | Ensure journald log file rotation is configured                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                              | Set Correctly            |                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                              | Yes                      | No                       |
| 6.2.1.1.4      | Ensure journald ForwardToSyslog is disabled                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.5      | Ensure journald Storage is configured                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.1.6      | Ensure journald Compress is configured                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.1      | Ensure systemd-journal-remote is installed                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.2      | Ensure systemd-journal-remote authentication is configured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.3      | Ensure systemd-journal-upload is enabled and active                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.1.2.4      | Ensure systemd-journal-remote service is not in use                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.1        | Ensure rsyslog is installed                                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.2        | Ensure rsyslog service is enabled and active                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.3        | Ensure all remote access methods are monitored                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.4        | Ensure journald is configured to send logs to rsyslog                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.5        | Ensure rsyslog log file creation mode is configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.6        | Ensure rsyslog logging is configured                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.7        | Ensure rsyslog is configured to send logs to a remote log host                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.8        | Ensure rsyslog is not configured to receive logs from a remote client                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.9        | Ensure logrotate is configured                                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.10       | Ensure rsyslog is configured to log cron events                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.11       | Ensure the rsyslog service is enabled and active                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.12       | Ensure the operating system has the packages required for encrypting offloaded audit logs                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.13       | Ensure the the operating system authenticates the remote logging server for off-loading audit logs                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.14       | Ensure the operating system encrypts audit records off-loaded onto a different system or media from the system being audited | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.2.15       | Ensure the audit system off-loads audit records onto a different system or media from the system being audited               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.1        | Ensure access to all logfiles has been configured                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.2        | Ensure /var/log/messages mode is configured                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.3        | Ensure /var/log/messages owner is configured                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                                                | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                                | Yes                      | No                       |
| 6.2.3.4        | Ensure /var/log/messages group owner is configured                                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.5        | Ensure /var/log is mode is configured                                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.6        | Ensure /var/log owner is configured                                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.7        | Ensure /var/log group owner is configured                                                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.2.3.8        | Ensure administrators are notified if an audit processing failure occurs by modifying /etc/aliases                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.1        | Ensure auditd packages are installed                                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.2        | Ensure auditing for processes that start prior to auditd is enabled                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.3        | Ensure audit_backlog_limit is sufficient                                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.4        | Ensure auditd service is enabled and active                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.5        | Ensure the operating system allocates a sufficient audit_backlog_limit to capture processes that start prior to the audit daemon                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.6        | Ensure the operating system's audit daemon is configured to include local events                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.7        | Ensure the operating system's audit daemon is configured to label all off-loaded audit logs                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.1.8        | Ensure the operating system's audit daemon is configured to resolve audit information before writing to disk                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.1        | Ensure audit log storage size is configured                                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.2        | Ensure audit logs are not automatically deleted                                                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.3        | Ensure system is disabled when audit logs are full                                                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.4        | Ensure system warns when audit logs are low on space                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.5        | Ensure the operating system allocates audit record storage capacity                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.6        | Ensure the SA and ISSO are notified in the event of an audit processing failure                                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.7        | Ensure the operating system notifies the SA and ISSO when allocated audit record storage volume reaches 75 percent                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.2.8        | Ensure the operating system takes action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                           | Set Correctly            |                          |
|----------------|-----------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                           | Yes                      | No                       |
| 6.3.2.9        | Ensure the audit system is configured to take an appropriate action when the internal event queue is full | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.1        | Ensure changes to system administration scope (sudoers) is collected                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.2        | Ensure actions as another user are always logged                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.3        | Ensure events that modify the sudo log file are collected                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.4        | Ensure events that modify date and time information are collected                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.5        | Ensure events that modify the system's network environment are collected                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.6        | Ensure use of privileged commands are collected                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.7        | Ensure unsuccessful file access attempts are collected                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.8        | Ensure events that modify user/group information are collected                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.9        | Ensure discretionary access control permission modification events are collected                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.10       | Ensure successful file system mounts are collected                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.11       | Ensure session initiation information is collected                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.12       | Ensure login and logout events are collected                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.13       | Ensure file deletion events by users are collected                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.14       | Ensure events that modify the system's Mandatory Access Controls are collected                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.15       | Ensure successful and unsuccessful attempts to use the chcon command are collected                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.16       | Ensure successful and unsuccessful attempts to use the setfacl command are collected                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.17       | Ensure successful and unsuccessful attempts to use the chacl command are collected                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.18       | Ensure successful and unsuccessful attempts to use the usermod command are collected                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.19       | Ensure kernel module loading unloading and modification is collected                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.20       | Ensure the audit configuration is immutable                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.21       | Ensure the running and on disk configuration is the same                                                  | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                  | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                  | Yes                      | No                       |
| 6.3.3.22       | Ensure successful and unsuccessful attempts to use the su command are collected                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.23       | Ensure successful and unsuccessful attempts to use the sudo command are collected                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.24       | Ensure successful and unsuccessful attempts to use the chsh command are collected                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.25       | Ensure successful and unsuccessful attempts to use the crontab command are collected             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.26       | Ensure successful and unsuccessful attempts to use the gpasswd command are collected             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.27       | Ensure successful and unsuccessful attempts to use the newgrp command are collected              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.28       | Ensure successful and unsuccessful attempts to use the pam_timestamp_check command are collected | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.29       | Ensure successful and unsuccessful attempts to use the ssh-keysign command are collected         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.30       | Ensure successful and unsuccessful attempts to use the unix_chkpwd command are collected         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.31       | Ensure successful and unsuccessful attempts to use the setsebool command are collected           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.32       | Ensure successful and unsuccessful attempts to use the userhelper command are collected          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.33       | Ensure successful and unsuccessful attempts to use the setfiles command are collected            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.34       | Ensure successful and unsuccessful attempts to use the semanage command are collected            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.35       | Ensure successful and unsuccessful attempts to use the postqueue command are collected           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.36       | Ensure successful and unsuccessful attempts to use the postdrop command are collected            | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.37       | Ensure successful and unsuccessful attempts to use the unix_update command are collected         | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.38       | Ensure successful and unsuccessful attempts to use the umount command are collected              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.39       | Ensure successful and unsuccessful attempts to use the mount command are collected               | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                        | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                        | Yes                      | No                       |
| 6.3.3.40       | Ensure successful and unsuccessful attempts to use the ssh-agent command are collected | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.41       | Ensure successful and unsuccessful attempts to use the passwd command are collected    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.42       | Ensure successful and unsuccessful attempts to use the chage command are collected     | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.43       | Ensure the audit system prevents unauthorized changes to logon UIDs                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.3.44       | Ensure successful and unsuccessful modifications to the faillock file are collected    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.1        | Ensure the audit log file directory mode is configured                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.2        | Ensure audit log files mode is configured                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.3        | Ensure audit log files owner is configured                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.4        | Ensure audit log files group owner is configured                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.5        | Ensure audit configuration files mode is configured                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.6        | Ensure audit configuration files owner is configured                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.7        | Ensure audit configuration files group owner is configured                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.8        | Ensure audit tools mode is configured                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.9        | Ensure audit tools owner is configured                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.10       | Ensure audit tools group owner is configured                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.11       | Ensure the audit logs are group-owned by root                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.12       | Ensure audit tools are mode 0755 or more restrictive                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.13       | Ensure the audit tools are owned by root                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.14       | Ensure audit tools are group owned by root                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.15       | Ensure the audit log file directories are mode 0700 or more restrictive                | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.16       | Ensure the audit log file directory is owned by root                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.17       | Ensure audit log files group owner is root                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.3.4.18       | Ensure audit log files are mode 0600 or more restrictive                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.1          | Ensure permissions on /etc/passwd are configured                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.2          | Ensure permissions on /etc/passwd- are configured                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.3          | Ensure permissions on /etc/group are configured                                        | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                           | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                           | Yes                      | No                       |
| 7.1.4          | Ensure permissions on /etc/group- are configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.5          | Ensure permissions on /etc/shadow are configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.6          | Ensure permissions on /etc/shadow- are configured                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.7          | Ensure permissions on /etc/gshadow are configured                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.8          | Ensure permissions on /etc/gshadow- are configured                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.9          | Ensure permissions on /etc/shells are configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.10         | Ensure permissions on /etc/security/opasswd are configured                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.11         | Ensure world writable files and directories are secured                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.12         | Ensure no files or directories without an owner and a group exist                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.13         | Ensure SUID and SGID files are reviewed                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.14         | Ensure there are no ".shosts" files on the operating system                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.15         | Ensure there are no "shosts.equiv" files on the operating system                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.16         | Ensure system-wide shared library directories have mode 755 or less permissive                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.17         | Ensure system-wide shared library directories must be owned by root                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.18         | Ensure the system-wide shared library directories are group-owned by root or a system account                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.19         | Ensure world-writable directories owner is configured                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.20         | Ensure world-writable directories group-owner is configured                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.21         | Ensure local initialization files do not execute world-writable programs                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.22         | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are mode 0755 or more restrictive | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.23         | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are owned by root                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.24         | Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are group-owned by root           | <input type="checkbox"/> | <input type="checkbox"/> |



| Recommendation |                                                                                                                                       | Set Correctly            |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                       | Yes                      | No                       |
| 7.1.25         | Ensure the system-wide shared library files are mode 0755 or more restrictive                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.26         | Ensure the system-wide shared library files are owned by root                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.1.27         | Ensure the system-wide shared library files are group-owned by root                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.1          | Ensure accounts in /etc/passwd use shadowed passwords                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.2          | Ensure /etc/shadow password fields are not empty                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.3          | Ensure all groups in /etc/passwd exist in /etc/group                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.4          | Ensure shadow group is empty                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.9          | Ensure local interactive user home directories are configured                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.10         | Ensure local interactive user dot files access is configured                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.11         | Ensure all files and directories in the local interactive user home directory are group-owned by a group that the user is a member of | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.12         | Ensure all files and directories in a local interactive user home directory are mode 0750 or more restrictive                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.13         | Ensure all local initialization files are mode 0740 or more restrictive                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.14         | Ensure local interactive user home directories group-owner is their primary GID                                                       | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: CIS Controls v8 Unmapped Recommendations

| Recommendation |                                                                                                  | Set Correctly            |                          |
|----------------|--------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                  | Yes                      | No                       |
| 1.2.2.3        | Ensure Operating System is a vendor-supported release                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.1          | Ensure message of the day is configured properly                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.2          | Ensure local login warning banner is configured properly                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.7.3          | Ensure remote login warning banner is configured properly                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.2          | Ensure GDM login banner is configured                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.8.3          | Ensure GDM disable-user-list option is enabled                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.3.3          | Ensure chrony is not run as the root user                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.4.1.1        | Ensure cron daemon is enabled and active                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.6          | Ensure sshd Banner is configured                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.8          | Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.11         | Ensure sshd HostbasedAuthentication is disabled                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.14         | Ensure sshd LoginGraceTime is configured                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.18         | Ensure sshd MaxSessions is configured                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.19         | Ensure sshd MaxStartups is configured                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.22         | Ensure sshd PermitUserEnvironment is disabled                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1.33         | Ensure sshd Banner is configured to display the Standard Mandatory DoD Notice and Consent Banner | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.1.1        | Ensure latest version of pam is installed                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.1.2        | Ensure latest version of authselect is installed                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3.2.5        | Ensure pam_unix module is enabled                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.1        | Ensure root is the only UID 0 account                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.2.5        | Ensure root path integrity                                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4.3.1        | Ensure nologin is not listed in /etc/shells                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 6.1.3          | Ensure cryptographic mechanisms are used to protect the integrity of audit tools                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.5          | Ensure no duplicate UIDs exist                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                       | Set Correctly            |                          |
|----------------|---------------------------------------|--------------------------|--------------------------|
|                |                                       | Yes                      | No                       |
| 7.2.6          | Ensure no duplicate GIDs exist        | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.7          | Ensure no duplicate user names exist  | <input type="checkbox"/> | <input type="checkbox"/> |
| 7.2.8          | Ensure no duplicate group names exist | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: Change History

| Date       | Version | Changes for this version |
|------------|---------|--------------------------|
| 11/16/2021 | 1.0.0   | PUBLISHED                |
|            |         |                          |

## ADDED ITEMS:

|            |       |                                                                                   |
|------------|-------|-----------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0 | ADDED RECOMMENDATION: 1.11 - Ensure the mailx package is installed                |
| 11/25/2024 | 2.0.0 | ADDED SECTION: 1.1 - Filesystem                                                   |
| 11/25/2024 | 2.0.0 | ADDED SECTION: 1.1.1 - Configure Filesystem Kernel Modules                        |
| 11/25/2024 | 2.0.0 | ADDED RECOMMENDATION: 1.1.1.1 - Ensure cramfs kernel module is not available      |
| 11/25/2024 | 2.0.0 | ADDED RECOMMENDATION: 1.1.1.2 - Ensure freevxfs kernel module is not available    |
| 11/25/2024 | 2.0.0 | ADDED RECOMMENDATION: 1.1.1.3 - Ensure hfs kernel module is not available         |
| 11/25/2024 | 2.0.0 | ADDED RECOMMENDATION: 1.1.1.4 - Ensure hfsplus kernel module is not available     |
| 11/25/2024 | 2.0.0 | ADDED RECOMMENDATION: 1.1.1.5 - Ensure jffs2 kernel module is not available       |
| 11/25/2024 | 2.0.0 | ADDED RECOMMENDATION: 1.1.1.6 - Ensure overlayfs kernel module is not available   |
| 11/25/2024 | 2.0.0 | ADDED RECOMMENDATION: 1.1.1.7 - Ensure squashfs kernel module is not available    |
| 11/25/2024 | 2.0.0 | ADDED RECOMMENDATION: 1.1.1.8 - Ensure udf kernel module is not available         |
| 11/25/2024 | 2.0.0 | ADDED RECOMMENDATION: 1.1.1.9 - Ensure usb-storage kernel module is not available |

| Date       | Version | Changes for this version                                                                                                    |
|------------|---------|-----------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.1.1.10 - Ensure unused filesystems kernel modules are not available                                 |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.1.2 - Configure Filesystem Partitions                                                                      |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.1.2.1 - Configure /tmp                                                                                     |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.1.2.1.1 - Ensure /tmp is a separate partition                                                       |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.1.2.2 - Configure /dev/shm                                                                                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.1.2.2.1 - Ensure /dev/shm is a separate partition                                                   |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.1.2.3 - Configure /home                                                                                    |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.1.2.3.3 - Ensure nosuid option set on /home partition                                               |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.1.2.3.5 - Ensure file systems that contain user home directories are mounted with the nosuid option |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.1.2.4 - Configure /var                                                                                     |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.1.2.4.2 - Ensure nodev option set on /var partition                                                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.1.2.4.3 - Ensure nosuid option set on /var partition                                                |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.1.2.5 - Configure /var/tmp                                                                                 |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.1.2.6 - Configure /var/log                                                                                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.1.2.6.2 - Ensure nodev option set on /var/log partition                                             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.1.2.6.3 - Ensure nosuid option set on /var/log partition                                            |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.1.2.6.4 - Ensure noexec option set on /var/log partition                                            |

| Date       | Version | Changes for this version                                                                                 |
|------------|---------|----------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.1.2.7 - Configure /var/log/audit                                                        |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.1.2.7.2 - Ensure nodev option set on /var/log/audit partition                    |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.1.2.7.3 - Ensure nosuid option set on /var/log/audit partition                   |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.1.2.7.4 - Ensure noexec option set on /var/log/audit partition                   |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.1.2.8 - Configure /boot                                                                 |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.1.2.9 - Configure /boot/efi                                                             |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.1.2.10 - Configure nfs filesystems                                                      |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.1.2.11 - Configure removable media partitions                                           |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.1.3 - Configure disk encryption                                                         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.1.3.1 - Ensure all information at rest is encrypted                              |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.2 - Package Management                                                                  |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.2.1 - Configure Package Repositories                                                    |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.2.1.3 - Ensure repo_gpgcheck is globally activated                               |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.2.1.6 - Ensure cryptographic verification of vendor software packages            |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.2.2 - Configure Package Updates                                                         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.2.2.2 - Ensure vendor packaged system security patches and updates are installed |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.2.2.3 - Ensure Operating System is a vendor-supported release                    |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.3.1.4 - Ensure the SELinux mode is not disabled                                  |

| Date       | Version | Changes for this version                                                                                          |
|------------|---------|-------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.3.1.5 - Ensure the SELinux mode is enforcing                                              |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.3.1.10 - Ensure SELinux prevents nonprivileged users from executing privileged functions  |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.3.1.11 - Ensure SELinux targeted policy is configured                                     |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.4 - Configure Bootloader                                                                         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.4.2 - Ensure access to bootloader config is configured                                    |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.4.5 - Ensure a unique name is set as the superusers account (BIOS)                        |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.4.6 - Ensure a unique name is set as the superusers account (UEFI)                        |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.5 - Configure Additional Process Hardening                                                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.5.1 - Ensure address space layout randomization is enabled                                |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.5.2 - Ensure ptrace_scope is restricted                                                   |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.5.3 - Ensure core dump backtraces are disabled                                            |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.5.4 - Ensure core dump storage is disabled                                                |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.5.5 - Ensure the storing of core dumps is disabled                                        |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.5.6 - Ensure the operating system is not configured to acquire save or process core dumps |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.6 - Configure system wide crypto policy                                                          |

| Date       | Version | Changes for this version                                                                                |
|------------|---------|---------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.6.1 - Ensure system wide crypto policy is not set to legacy                     |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.6.2 - Ensure system wide crypto policy is not set in sshd configuration         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.6.3 - Ensure system wide crypto policy disables sha1 hash and signature support |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.6.4 - Ensure system wide crypto policy disables macs less than 128 bits         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.6.5 - Ensure system wide crypto policy disables cbc for ssh                     |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.6.6 - Ensure system wide crypto policy disables chacha20-poly1305 for ssh       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.6.7 - Ensure system wide crypto policy disables EtM for ssh                     |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.6.8 - Ensure system-wide crypto policy is FIPS                                  |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.7 - Configure Command Line Warning Banners                                             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.7.4 - Ensure access to /etc/motd is configured                                  |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.7.5 - Ensure access to /etc/issue is configured                                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.7.6 - Ensure access to /etc/issue.net is configured                             |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 1.8 - Configure GNOME Display Manager                                                    |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.8.3 - Ensure GDM disable-user-list option is enabled                            |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.8.4 - Ensure GDM screen locks when the user is idle                             |



| Date       | Version | Changes for this version                                                                                                                                   |
|------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.8.5 - Ensure GDM screen locks cannot be overridden                                                                                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.8.6 - Ensure GDM automatic mounting of removable media is disabled                                                                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.8.7 - Ensure GDM disabling automatic mounting of removable media is not overridden                                                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.8.9 - Ensure GDM autorun-never is enabled                                                                                          |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.8.11 - Ensure GDM autorun-never is not overridden                                                                                  |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.8.13 - Ensure XDMCP is not enabled                                                                                                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.8.15 - Ensure GDM login banner displays the Mandatory DoD Notice and Consent Banner                                                |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 1.8.18 - Ensure the operating system initiates a session lock for all connection types using smartcard when the smartcard is removed |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 2.1 - Configure Server Services                                                                                                             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.1 - Ensure autofs services are not in use                                                                                        |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.2 - Ensure avahi daemon services are not in use                                                                                  |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.3 - Ensure dhcp server services are not in use                                                                                   |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.4 - Ensure dns server services are not in use                                                                                    |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.5 - Ensure dnsmasq services are not in use                                                                                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.6 - Ensure ftp server services are not in use                                                                                    |

| Date       | Version | Changes for this version                                                                          |
|------------|---------|---------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.7 - Ensure message access server services are not in use                |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.8 - Ensure network file system services are not in use                  |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.9 - Ensure nis server services are not in use                           |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.10 - Ensure print server services are not in use                        |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.11 - Ensure rpcbind services are not in use                             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.12 - Ensure rsync services are not in use                               |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.13 - Ensure samba file server services are not in use                   |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.14 - Ensure snmp services are not in use                                |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.15 - Ensure telnet server services are not in use                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.16 - Ensure tftp server services are not in use                         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.17 - Ensure web proxy server services are not in use                    |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.18 - Ensure web server services are not in use                          |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.19 - Ensure xinetd services are not in use                              |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.20 - Ensure X window server services are not in use                     |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.21 - Ensure only approved services are listening on a network interface |

| Date       | Version | Changes for this version                                                                                  |
|------------|---------|-----------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.23 - Ensure mail transfer agents are configured for local-only mode             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.1.26 - Ensure system daemons are prevented from using Kerberos for authentication |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 2.2 - Configure Client Services                                                            |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.2.1 - Ensure ftp client is not installed                                          |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.2.2 - Ensure ldap client is not installed                                         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.2.3 - Ensure nis client is not installed                                          |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.2.5 - Ensure tftp client is not installed                                         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.2.6 - Ensure krb5-workstation is not installed                                    |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 2.3 - Configure Time Synchronization                                                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.3.3 - Ensure chrony is not run as the root user                                   |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 2.4 - Job Schedulers                                                                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.4.1.1 - Ensure cron daemon is enabled and active                                  |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.4.1.8 - Ensure crontab is restricted to authorized users                          |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 2.4.2 - Configure at                                                                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.4.2.1 - Ensure at is restricted to authorized users                               |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 2.5 - Configure USBGuard                                                                   |

| Date       | Version | Changes for this version                                                                      |
|------------|---------|-----------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.5.4 - Ensure the usbguard service is enabled and active               |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 2.6 - Configure fapolicyd                                                      |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.6.1 - Ensure fapolicyd is installed                                   |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.6.2 - Ensure fapolicyd employs a deny-all, permit-by-exception policy |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 2.6.3 - Ensure fapolicyd is enabled and running                         |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 3 - Network                                                                    |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 3.1 - Configure Network Devices                                                |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 3.1.1 - Ensure IPv6 status is identified                                |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 3.1.3 - Ensure bluetooth services are not in use                        |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 3.2 - Configure Network Kernel Modules                                         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 3.2.1 - Ensure dccp kernel module is not available                      |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 3.2.2 - Ensure tipc kernel module is not available                      |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 3.2.3 - Ensure rds kernel module is not available                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 3.2.4 - Ensure sctp kernel module is not available                      |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 3.2.5 - Ensure atm kernel module is not available                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 3.2.6 - Ensure bluetooth kernel module is not available                 |

| Date       | Version | Changes for this version                                                               |
|------------|---------|----------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 3.2.7 - Ensure can kernel module is not available                |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 3.3 - Configure Network Kernel Parameters                               |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 3.3.1 - Ensure ip forwarding is disabled                         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 3.3.3 - Ensure bogus icmp responses are ignored                  |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 3.3.4 - Ensure broadcast icmp requests are ignored               |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 3.3.5 - Ensure icmp redirects are not accepted                   |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 3.3.6 - Ensure secure icmp redirects are not accepted            |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 3.3.7 - Ensure reverse path filtering is enabled                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 3.3.10 - Ensure tcp syn cookies is enabled                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 3.3.11 - Ensure ipv6 router advertisements are not accepted      |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 3.3.12 - Ensure net.ipv4.conf.all.forwarding is disabled         |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 4 - Host Based Firewall                                                 |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 4.1 - Configure a firewall utility                                      |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 4.1.4 - Ensure nftables is installed                             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 4.1.5 - Ensure a single firewall configuration utility is in use |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 4.1.1 - Configure firewall rules                                        |

| Date       | Version | Changes for this version                                                                             |
|------------|---------|------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 4.1.1.2 - Ensure host based firewall loopback traffic is configured            |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 4.1.1.4 - Ensure nftables established connections are configured               |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 5 - Access Control                                                                    |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 5.1 - Configure SSH Server                                                            |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.1 - Ensure openssh-server is installed                                     |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.5 - Ensure sshd access is configured                                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.6 - Ensure sshd Banner is configured                                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.7 - Ensure sshd Ciphers are configured                                     |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.8 - Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.9 - Ensure sshd DisableForwarding is enabled                               |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.10 - Ensure sshd GSSAPIAuthentication is disabled                          |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.11 - Ensure sshd HostbasedAuthentication is disabled                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.12 - Ensure sshd IgnoreRhosts is enabled                                   |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.13 - Ensure sshd KexAlgorithms is configured                               |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.14 - Ensure sshd LoginGraceTime is configured                              |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.15 - Ensure sshd LogLevel is configured                                    |

| Date       | Version | Changes for this version                                                                                    |
|------------|---------|-------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.16 - Ensure sshd MACs are configured                                              |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.17 - Ensure sshd MaxAuthTries is configured                                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.18 - Ensure sshd MaxSessions is configured                                        |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.19 - Ensure sshd MaxStartups is configured                                        |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.20 - Ensure sshd PermitEmptyPasswords is disabled                                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.21 - Ensure sshd PermitRootLogin is disabled                                      |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.22 - Ensure sshd PermitUserEnvironment is disabled                                |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.23 - Ensure sshd UsePAM is enabled                                                |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.24 - Ensure sshd private key files have a passcode                                |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.25 - Ensure sshd X11Forwarding is disabled                                        |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.26 - Ensure sshd ClientAliveInterval is configured                                |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.27 - Ensure sshd ClientAliveCountMax is configured                                |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.30 - Ensure sshd is configured to use only FIPS-validated key exchange algorithms |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.32 - Ensure sshd StrictModes is enabled                                           |

| Date       | Version | Changes for this version                                                                                                        |
|------------|---------|---------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.33 - Ensure sshd Banner is configured to display the Standard Mandatory DoD Notice and Consent Banner |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.34 - Ensure sshd IgnoreUserKnownHosts is enabled                                                      |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.35 - Ensure sshd X11UseLocalhost is enabled                                                           |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.36 - Ensure sshd KerberosAuthentication is disabled                                                   |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.37 - Ensure sshd RekeyLimit is configured                                                             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.1.38 - Ensure sshd PrintLastLog is enabled                                                              |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 5.2 - Configure privilege escalation                                                                             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.2.2 - Ensure the sudoers file has the default include directory                                         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.2.5 - Ensure users must provide password for escalation                                                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.2.6 - Ensure the sudoers file restricts sudo access to authorized personnel                             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.2.7 - Ensure re-authentication for privilege escalation is not disabled globally                        |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.2.9 - Ensure sudo timestamp_timeout is configured                                                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.2.11 - Ensure pam_succeed_if does not exist in /etc/pam.d/sudo                                          |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 5.3 - Pluggable Authentication Modules                                                                           |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 5.3.1 - Configure PAM software packages                                                                          |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.1.1 - Ensure latest version of pam is installed                                                       |



| Date       | Version | Changes for this version                                                                            |
|------------|---------|-----------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.1.2 - Ensure latest version of authselect is installed                    |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.2.1 - Ensure active authselect profile includes pam modules               |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.2.2 - Ensure pam_faillock module is enabled                               |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.2.3 - Ensure pam_pwquality module is enabled                              |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.2.4 - Ensure pam_pwhistory module is enabled                              |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.2.5 - Ensure pam_unix module is enabled                                   |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 5.3.3 - Configure PAM Arguments                                                      |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 5.3.3.1 - Configure pam_faillock module                                              |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.1.1 - Ensure password failed attempts lockout is configured             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.1.2 - Ensure password unlock time is configured                         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.1.3 - Ensure password failed attempts lockout includes root account     |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.1.4 - Ensure deny is configured on the pam_faillock module              |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.1.5 - Ensure deny is configured in /etc/security/faillock.conf          |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.1.6 - Ensure fail_interval is configured on the pam_faillock module     |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.1.7 - Ensure fail_interval is configured in /etc/security/faillock.conf |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.1.8 - Ensure unlock_time is configured on the pam_faillock module       |

| Date       | Version | Changes for this version                                                                                                                                        |
|------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.1.9 - Ensure unlock_time is configured in /etc/security/faillock.conf                                                               |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.1.10 - Ensure dir is configured on the pam_faillock module                                                                          |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.1.11 - Ensure dir is configured in /etc/security/faillock.conf                                                                      |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.1.12 - Ensure silent is set on the pam_faillock module                                                                              |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.1.13 - Ensure silent is set in /etc/security/faillock.conf                                                                          |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.1.14 - Ensure audit is set on the pam_faillock module                                                                               |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.1.15 - Ensure audit is set in /etc/security/faillock.conf                                                                           |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.1.16 - Ensure even_deny_root is set on the pam_faillock module                                                                      |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.1.17 - Ensure even_deny_root is set in /etc/security/faillock.conf                                                                  |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.1.18 - Ensure the use of a non-default faillock tally directory while SELinux enforces a targeted policy                            |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.1.19 - Ensure the use of a non-default faillock tally directory on the pam_faillock module while SELinux enforces a targeted policy |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 5.3.3.2 - Configure pam_pwquality module                                                                                                         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.2.1 - Ensure password number of changed characters is configured                                                                    |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.2.2 - Ensure password length is configured                                                                                          |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.2.3 - Ensure password complexity is configured                                                                                      |

| Date       | Version | Changes for this version                                                                                              |
|------------|---------|-----------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.2.4 - Ensure password same consecutive characters is configured                           |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.2.5 - Ensure password maximum sequential characters is configured                         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.2.6 - Ensure password dictionary check is enabled                                         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.2.7 - Ensure password quality is enforced for the root user                               |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.2.9 - Ensure ucredit is configured in /etc/security/pwquality.conf                        |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.2.10 - Ensure lcredit is configured in /etc/security/pwquality.conf                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.2.11 - Ensure dcredit is configured in /etc/security/pwquality.conf                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.2.12 - Ensure ocredit is configured in /etc/security/pwquality.conf                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.2.13 - Ensure maxclassrepeat is configured in /etc/security/pwquality.conf                |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.2.14 - Ensure minclass is configured in /etc/security/pwquality.conf                      |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.2.15 - Ensure difok is configured in /etc/security/pwquality.conf                         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.2.16 - Ensure dictcheck is configured                                                     |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.2.17 - Ensure retry is configured on the pam_pwquality module in /etc/pam.d/system-auth   |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.2.18 - Ensure retry is configured on the pam_pwquality module in /etc/pam.d/password-auth |

| Date       | Version | Changes for this version                                                                                                |
|------------|---------|-------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.2.19 - Ensure retry is configured in /etc/security/pwquality.conf                           |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 5.3.3.3 - Configure pam_pwhistory module                                                                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.3.1 - Ensure password history remember is configured                                        |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.3.2 - Ensure password history is enforced for the root user                                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.3.3 - Ensure pam_pwhistory includes use_authok                                              |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.3.4 - Ensure remember is configured on the pam_pwhistory module in /etc/pam.d/password-auth |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.3.5 - Ensure remember is configured on the pam_pwhistory module in /etc/pam.d/system-auth   |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 5.3.3.4 - Configure pam_unix module                                                                      |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.4.1 - Ensure pam_unix does not include nullok                                               |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.4.2 - Ensure pam_unix does not include remember                                             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.4.3 - Ensure pam_unix includes a strong password hashing algorithm                          |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.4.4 - Ensure pam_unix includes use_authok                                                   |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.3.3.4.5 - Ensure pam_unix includes a FIPS 140-2 approved hashing algorithm                      |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 5.3.3.5 - Configure pam_lastlog module                                                                   |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 5.3.3.6 - Configure pam_sss module                                                                       |

| Date       | Version | Changes for this version                                                                                          |
|------------|---------|-------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED SECTION: 5.4.1 - Configure shadow password suite parameters                                                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.1.1 - Ensure password expiration is configured                                          |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.1.2 - Ensure minimum password days is configured                                        |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.1.3 - Ensure password expiration warning days is configured                             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.1.4 - Ensure strong password hashing algorithm is configured                            |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.1.5 - Ensure inactive password lock is configured                                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.1.7 - Ensure passwords use FIPS 140-2 approved cryptographic hashing algorithm          |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.1.8 - Ensure minimum number of hashing rounds is configured                             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.1.9 - Ensure existing passwords use FIPS 140-2 approved cryptographic hashing algorithm |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.1.11 - Ensure fail_delay is configured                                                  |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.1.12 - Ensure pass_min_len is configured                                                |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 5.4.2 - Configure root and system accounts and environment                                         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.2.2 - Ensure root is the only GID 0 account                                             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.2.3 - Ensure group root is the only GID 0 group                                         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.2.4 - Ensure root account access is controlled                                          |

| Date       | Version | Changes for this version                                                                                                        |
|------------|---------|---------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.2.5 - Ensure root path integrity                                                                      |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.2.6 - Ensure root user umask is configured                                                            |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.2.7 - Ensure system accounts do not have a valid login shell                                          |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.2.8 - Ensure accounts without a valid login shell are locked                                          |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 5.4.3 - Configure user default environment                                                                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.3.1 - Ensure nologin is not listed in /etc/shells                                                     |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.3.2 - Ensure default user shell timeout is configured                                                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.3.3 - Ensure default user umask is configured                                                         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.3.14 - Ensure the number of concurrent sessions is configured                                         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 5.4.3.16 - Ensure StopIdleSessionSec is configured                                                        |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 6.1 - Configure Integrity Checking                                                                               |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.1.3 - Ensure cryptographic mechanisms are used to protect the integrity of audit tools                  |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.1.4 - Ensure AIDE is configured to use cryptographic mechanisms to protect the integrity of audit tools |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 6.2 - System Logging                                                                                             |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 6.2.1.1 - Configure systemd-journald service                                                                     |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.1.1.1 - Ensure journald service is enabled and active                                                 |

| Date       | Version | Changes for this version                                                                              |
|------------|---------|-------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.1.1.2 - Ensure journald log file access is configured                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.1.1.3 - Ensure journald log file rotation is configured                     |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.1.1.4 - Ensure journald ForwardToSyslog is disabled                         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.1.1.5 - Ensure journald Storage is configured                               |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.1.1.6 - Ensure journald Compress is configured                              |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 6.2.1.2 - Configure systemd-journal-remote                                             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.1.2.1 - Ensure systemd-journal-remote is installed                          |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.1.2.2 - Ensure systemd-journal-remote authentication is configured          |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.1.2.3 - Ensure systemd-journal-upload is enabled and active                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.1.2.4 - Ensure systemd-journal-remote service is not in use                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.2.2 - Ensure rsyslog service is enabled and active                          |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.2.3 - Ensure all remote access methods are monitored                        |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.2.5 - Ensure rsyslog log file creation mode is configured                   |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.2.6 - Ensure rsyslog logging is configured                                  |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.2.8 - Ensure rsyslog is not configured to receive logs from a remote client |

| Date       | Version | Changes for this version                                                                                                           |
|------------|---------|------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.2.10 - Ensure rsyslog is configured to log cron events                                                   |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 6.2.3 - Configure Logfiles                                                                                          |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.3.1 - Ensure access to all logfiles has been configured                                                  |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.3.2 - Ensure /var/log/messages mode is configured                                                        |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.3.3 - Ensure /var/log/messages owner is configured                                                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.3.4 - Ensure /var/log/messages group owner is configured                                                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.3.5 - Ensure /var/log is mode is configured                                                              |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.3.6 - Ensure /var/log owner is configured                                                                |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.3.7 - Ensure /var/log group owner is configured                                                          |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.2.3.8 - Ensure administrators are notified if an audit processing failure occurs by modifying /etc/aliases |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 6.3 - System Auditing                                                                                               |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 6.3.1 - Configure auditd Service                                                                                    |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.1.1 - Ensure auditd packages are installed                                                               |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.1.4 - Ensure auditd service is enabled and active                                                        |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.2.4 - Ensure system warns when audit logs are low on space                                               |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 6.3.3 - Configure auditd Rules                                                                                      |



| Date       | Version | Changes for this version                                                                                              |
|------------|---------|-----------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.2 - Ensure actions as another user are always logged                                      |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.3 - Ensure events that modify the sudo log file are collected                             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.6 - Ensure use of privileged commands are collected                                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.7 - Ensure unsuccessful file access attempts are collected                                |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.15 - Ensure successful and unsuccessful attempts to use the chcon command are collected   |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.16 - Ensure successful and unsuccessful attempts to use the setfacl command are collected |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.17 - Ensure successful and unsuccessful attempts to use the chacl command are collected   |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.18 - Ensure successful and unsuccessful attempts to use the usermod command are collected |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.19 - Ensure kernel module loading unloading and modification is collected                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.21 - Ensure the running and on disk configuration is the same                             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.22 - Ensure successful and unsuccessful attempts to use the su command are collected      |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.23 - Ensure successful and unsuccessful attempts to use the sudo command are collected    |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.24 - Ensure successful and unsuccessful attempts to use the chsh command are collected    |

| Date       | Version | Changes for this version                                                                                                          |
|------------|---------|-----------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.25 - Ensure successful and unsuccessful attempts to use the crontab command are collected             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.26 - Ensure successful and unsuccessful attempts to use the gpasswd command are collected             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.27 - Ensure successful and unsuccessful attempts to use the newgrp command are collected              |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.28 - Ensure successful and unsuccessful attempts to use the pam_timestamp_check command are collected |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.29 - Ensure successful and unsuccessful attempts to use the ssh-keysign command are collected         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.30 - Ensure successful and unsuccessful attempts to use the unix_chkpwd command are collected         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.31 - Ensure successful and unsuccessful attempts to use the setsebool command are collected           |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.32 - Ensure successful and unsuccessful attempts to use the userhelper command are collected          |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.33 - Ensure successful and unsuccessful attempts to use the setfiles command are collected            |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.34 - Ensure successful and unsuccessful attempts to use the semanage command are collected            |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.35 - Ensure successful and unsuccessful attempts to use the postqueue command are collected           |

| Date       | Version | Changes for this version                                                                                                  |
|------------|---------|---------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.36 - Ensure successful and unsuccessful attempts to use the postdrop command are collected    |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.37 - Ensure successful and unsuccessful attempts to use the unix_update command are collected |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.38 - Ensure successful and unsuccessful attempts to use the umount command are collected      |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.39 - Ensure successful and unsuccessful attempts to use the mount command are collected       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.40 - Ensure successful and unsuccessful attempts to use the ssh-agent command are collected   |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.41 - Ensure successful and unsuccessful attempts to use the passwd command are collected      |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.42 - Ensure successful and unsuccessful attempts to use the chage command are collected       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.3.44 - Ensure successful and unsuccessful modifications to the faillock file are collected      |
| 11/25/2024 | 2.0.0   | ADDED SECTION: 6.3.4 - Configure auditd File Access                                                                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.4.1 - Ensure the audit log file directory mode is configured                                    |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.4.2 - Ensure audit log files mode is configured                                                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.4.3 - Ensure audit log files owner is configured                                                |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.4.4 - Ensure audit log files group owner is configured                                          |

| Date       | Version | Changes for this version                                                                                 |
|------------|---------|----------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.4.5 - Ensure audit configuration files mode is configured                      |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.4.6 - Ensure audit configuration files owner is configured                     |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.4.7 - Ensure audit configuration files group owner is configured               |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.4.8 - Ensure audit tools mode is configured                                    |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.4.9 - Ensure audit tools owner is configured                                   |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.4.10 - Ensure audit tools group owner is configured                            |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.4.11 - Ensure the audit logs are group-owned by root                           |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.4.12 - Ensure audit tools are mode 0755 or more restrictive                    |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.4.13 - Ensure the audit tools are owned by root                                |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.4.14 - Ensure audit tools are group owned by root                              |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.4.15 - Ensure the audit log file directories are mode 0700 or more restrictive |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.4.16 - Ensure the audit log file directory is owned by root                    |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.4.17 - Ensure audit log files group owner is root                              |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 6.3.4.18 - Ensure audit log files are mode 0600 or more restrictive                |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 7.1.9 - Ensure permissions on /etc/shells are configured                           |

| Date       | Version | Changes for this version                                                                                                                                 |
|------------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 7.1.10 - Ensure permissions on /etc/security/opasswd are configured                                                                |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 7.1.11 - Ensure world writable files and directories are secured                                                                   |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 7.1.12 - Ensure no files or directories without an owner and a group exist                                                         |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 7.1.13 - Ensure SUID and SGID files are reviewed                                                                                   |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 7.1.16 - Ensure system-wide shared library directories have mode 755 or less permissive                                            |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 7.1.17 - Ensure system-wide shared library directories must be owned by root                                                       |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 7.1.18 - Ensure the system-wide shared library directories are group-owned by root or a system account                             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 7.1.19 - Ensure world-writable directories owner is configured                                                                     |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 7.1.20 - Ensure world-writable directories group-owner is configured                                                               |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 7.1.22 - Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are mode 0755 or more restrictive |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 7.1.23 - Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are owned by root                 |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 7.1.24 - Ensure the /bin /sbin /usr/bin /usr/sbin /usr/local/bin and /usr/local/sbin directories are group-owned by root           |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 7.1.25 - Ensure the system-wide shared library files are mode 0755 or more restrictive                                             |
| 11/25/2024 | 2.0.0   | ADDED RECOMMENDATION: 7.1.26 - Ensure the system-wide shared library files are owned by root                                                             |

| Date           | Version | Changes for this version                                                                                                                          |
|----------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024     | 2.0.0   | ADDED RECOMMENDATION: 7.1.27 - Ensure the system-wide shared library files are group-owned by root                                                |
| 11/25/2024     | 2.0.0   | ADDED SECTION: 7.2 - Local User and Group Settings                                                                                                |
| 11/25/2024     | 2.0.0   | ADDED RECOMMENDATION: 7.2.1 - Ensure accounts in /etc/passwd use shadowed passwords                                                               |
| 11/25/2024     | 2.0.0   | ADDED RECOMMENDATION: 7.2.2 - Ensure /etc/shadow password fields are not empty                                                                    |
| 11/25/2024     | 2.0.0   | ADDED RECOMMENDATION: 7.2.9 - Ensure local interactive user home directories are configured                                                       |
| 11/25/2024     | 2.0.0   | ADDED RECOMMENDATION: 7.2.10 - Ensure local interactive user dot files access is configured                                                       |
| 11/25/2024     | 2.0.0   | ADDED RECOMMENDATION: 7.2.12 - Ensure all files and directories in a local interactive user home directory are mode 0750 or more restrictive      |
| 11/25/2024     | 2.0.0   | ADDED RECOMMENDATION: 7.2.13 - Ensure all local initialization files are mode 0740 or more restrictive                                            |
| 11/25/2024     | 2.0.0   | ADDED RECOMMENDATION: 7.2.14 - Ensure local interactive user home directories group-owner is their primary GID                                    |
| DROPPED ITEMS: |         |                                                                                                                                                   |
| 11/25/2024     | 2.0.0   | DROPPED RECOMMENDATION: 1.11 - Ensure system-wide crypto policy is not legacy                                                                     |
| 11/25/2024     | 2.0.0   | DROPPED RECOMMENDATION: 1.12 - Ensure system-wide crypto policy is FUTURE or FIPS                                                                 |
| 11/25/2024     | 2.0.0   | DROPPED RECOMMENDATION: 1.13 - Ensure the operating system implements DoD-approved encryption                                                     |
| 11/25/2024     | 2.0.0   | DROPPED RECOMMENDATION: 1.14 - Ensure the operating system prevents unauthorized modification of all information at rest by using disk encryption |

| Date       | Version | Changes for this version                                                                                                      |
|------------|---------|-------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.29 - Ensure the operating system disables the ability to load the USB Storage kernel module         |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 1.1 - Filesystem Configuration                                                                               |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.1.2 - Ensure /tmp is configured                                                                     |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.1.21 - Ensure sticky bit is set on all world-writable directories                                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.1.22 - Disable Automounting                                                                         |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.1.23 - Disable USB Storage                                                                          |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.1.24 - Ensure file systems that contain user home directories are mounted with the "nosuid" option" |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.1.31 - Ensure /var/log" is mounted with the "nodev" option"                                         |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.1.32 - Ensure /var/log" is mounted with the "nosuid" option"                                        |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.1.33 - Ensure /var/log" is mounted with the "noexec" option"                                        |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.1.34 - Ensure /var/log/audit" is mounted with the "nodev" option"                                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.1.35 - Ensure /var/log/audit" is mounted with the "nosuid" option"                                  |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.1.36 - Ensure /var/log/audit" is mounted with the "noexec" option"                                  |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 1.1.1 - Disable unused filesystems                                                                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.1.1.1 - Ensure mounting of cramfs filesystems is disabled                                           |

| Date       | Version | Changes for this version                                                                                                                                                              |
|------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.1.1.2 - Ensure mounting of vFAT filesystems is limited                                                                                                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.1.1.3 - Ensure mounting of squashfs filesystems is disabled                                                                                                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.1.1.4 - Ensure mounting of udf filesystems is disabled                                                                                                      |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 1.2 - Configure Software Updates                                                                                                                                     |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 1.3 - Configure sudo                                                                                                                                                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.3.4 - Ensure the /etc/sudoers" file has no occurrences of "NOPASSWD""                                                                                       |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.3.5 - Ensure the /etc/sudoers" file has no occurrences of "!authenticate""                                                                                  |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.3.6 - Ensure the sudoers" file restricts sudo access to authorized personnel"                                                                               |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.3.8 - Ensure the operating system requires re-authentication when using the sudo" command to elevate privileges"                                            |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 1.4 - Filesystem Integrity Checking                                                                                                                                  |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.4.3 - Ensure Advanced Intrusion Detection Environment (AIDE) is properly configured to use cryptographic mechanisms to protect the integrity of audit tools |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 1.5 - Secure Boot Settings                                                                                                                                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.5.1 - Ensure permissions on bootloader config are configured                                                                                                |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.5.3 - Ensure authentication required for single user mode                                                                                                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.5.4 - Ensure the encrypted grub superusers password is set for systems booted with UEFI                                                                     |



| Date       | Version | Changes for this version                                                                                              |
|------------|---------|-----------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.5.5 - Ensure the encrypted grub superusers password is set for system booted with BIOS      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.5.13 - Ensure a unique name is set as the superusers" account (UEFI)"                       |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.5.14 - Ensure a unique name is set as the superusers" account (BIOS)"                       |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 1.6 - Additional Process Hardening                                                                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.6.1 - Ensure core dumps are restricted                                                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.6.2 - Ensure address space layout randomization (ASLR) is enabled                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.6.3 - Ensure the operating system disables the storing core dumps                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.6.4 - Ensure the operating system is not configured to acquire, save, or process core dumps |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.6.7 - Ensure the operating system disables storing core dumps for all users                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.6.8 - Ensure the operating system disables core dump backtraces                             |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.7.1.4 - Ensure the SELinux state is enforcing                                               |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 1.8 - Command Line Warning Banners                                                                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.8.5 - Ensure permissions on /etc/motd are configured                                        |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.8.6 - Ensure permissions on /etc/issue are configured                                       |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.8.7 - Ensure permissions on /etc/issue.net are configured                                   |

| Date       | Version | Changes for this version                                                                                                                                                                            |
|------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.8.8 - Ensure the Standard Mandatory DoD Notice and Consent Banner is displayed before granting access to the system via SSH logon                                         |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.8.9 - Ensure the operating system displays a banner before granting access to the operating system via a graphical user logon                                             |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 1.9 - GNOME Display Manager                                                                                                                                                        |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.9.1 - Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a graphical user logon |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.9.4 - Ensure last logged in user display is disabled                                                                                                                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.9.5 - Ensure XDCMP is not enabled                                                                                                                                         |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 1.9.6 - Ensure a Standard Mandatory DoD Notice and Consent Banner is displayed via a graphical user logon                                                                   |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 2.1 - inetd Services                                                                                                                                                               |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.1.1 - Ensure xinetd is not installed                                                                                                                                      |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 2.2 - Special Purpose Services                                                                                                                                                     |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.2.2 - Ensure X Window System is not installed                                                                                                                             |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.2.3 - Ensure rsync service is not enabled                                                                                                                                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.2.4 - Ensure Avahi Server is not enabled                                                                                                                                  |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.2.5 - Ensure SNMP Server is not enabled                                                                                                                                   |

| Date       | Version | Changes for this version                                                                      |
|------------|---------|-----------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.2.6 - Ensure HTTP Proxy Server is not enabled                       |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.2.7 - Ensure Samba is not enabled                                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.2.8 - Ensure IMAP and POP3 server is not enabled                    |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.2.9 - Ensure HTTP server is not enabled                             |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.2.10 - Ensure FTP Server is not enabled                             |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.2.11 - Ensure DNS Server is not enabled                             |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.2.12 - Ensure NFS is not enabled                                    |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.2.13 - Ensure RPC is not enabled                                    |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.2.14 - Ensure LDAP server is not enabled                            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.2.15 - Ensure DHCP Server is not enabled                            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.2.16 - Ensure the telnet-server package is not installed            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.2.17 - Ensure CUPS is not enabled                                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.2.18 - Ensure NIS Server is not enabled                             |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.2.19 - Ensure mail transfer agent is configured for local-only mode |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.2.29 - Ensure an FTP server has not been installed on the system    |

| Date       | Version | Changes for this version                                                                                                                             |
|------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 2.2.1 - Time Synchronization                                                                                                        |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 2.3 - Service Clients                                                                                                               |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.3.1 - Ensure NIS Client is not installed                                                                                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 2.3.3 - Ensure LDAP client is not installed                                                                                  |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 3 - Network Configuration                                                                                                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.6 - Disable IPv6                                                                                                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.8 - Ensure Bluetooth is disabled                                                                                           |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 3.1 - Network Parameters (Host Only)                                                                                                |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.1.1 - Ensure IP forwarding is disabled                                                                                     |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.1.3 - Ensure the system does not accept router advertisements on IPv6 interfaces, unless the system is a router            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.1.4 - Ensure the system does not accept router advertisements on IPv6 interfaces by default, unless the system is a router |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 3.2 - Network Parameters (Host and Router)                                                                                          |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.2.2 - Ensure ICMP redirects are not accepted                                                                               |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.2.3 - Ensure secure ICMP redirects are not accepted                                                                        |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.2.5 - Ensure broadcast ICMP requests are ignored                                                                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.2.6 - Ensure bogus ICMP responses are ignored                                                                              |

| Date       | Version | Changes for this version                                                                                           |
|------------|---------|--------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.2.7 - Ensure Reverse Path Filtering is enabled                                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.2.8 - Ensure TCP SYN Cookies is enabled                                                  |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.2.9 - Ensure IPv6 router advertisements are not accepted                                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.2.10 - Ensure the operating system does not accept IPv6 ICMP redirect messages           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.2.11 - Ensure the operating system does not accept IPv6 source-routed packets            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.2.12 - Ensure the operating system does not accept IPv6 source-routed packets by default |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.2.13 - Ensure the operating system ignores IPv6 ICMP redirect messages                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.2.15 - Ensure the operating system does not accept IPv4 ICMP redirect messages           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.2.16 - Ensure the operating system does not accept IPv4 source-routed packet             |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.2.17 - Ensure the operating system does not accept IPv4 source-routed packets by default |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.2.18 - Ensure the operating system ignores IPv4 ICMP redirect messages                   |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 3.3 - Uncommon Network Protocols                                                                  |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.3.1 - Ensure DCCP is disabled                                                            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.3.2 - Ensure SCTP is disabled                                                            |

| Date       | Version | Changes for this version                                                                     |
|------------|---------|----------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.3.3 - Ensure RDS is disabled                                       |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.3.4 - Ensure TIPC is disabled                                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.3.5 - Ensure ATM is disabled                                       |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.3.6 - Ensure CAN is disabled                                       |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 3.4 - Firewall Configuration                                                |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 3.4.1 - Ensure Firewall software is installed                               |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.1.1 - Ensure a Firewall package is installed                     |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 3.4.2 - Configure firewalld                                                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.2.2 - Ensure iptables service is not enabled with firewalld      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.2.3 - Ensure nftables is not enabled with firewalld              |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.2.4 - Ensure firewalld default zone is set                       |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.2.5 - Ensure network interfaces are assigned to appropriate zone |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 3.4.3 - Configure nftables                                                  |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.3.1 - Ensure iptables are flushed with nftables                  |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.3.2 - Ensure an nftables table exists                            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.3.4 - Ensure nftables loopback traffic is configured             |

| Date       | Version | Changes for this version                                                                                 |
|------------|---------|----------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.3.5 - Ensure nftables outbound and established connections are configured    |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.3.7 - Ensure nftables service is enabled                                     |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.3.8 - Ensure nftables rules are permanent                                    |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 3.4.4 - Configure iptables                                                              |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 3.4.4.1 - Configure IPv4 iptables                                                       |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.4.1.1 - Ensure iptables loopback traffic is configured                       |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.4.1.2 - Ensure iptables outbound and established connections are configured  |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.4.1.3 - Ensure iptables firewall rules exist for all open ports              |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.4.1.4 - Ensure iptables default deny firewall policy                         |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.4.1.5 - Ensure iptables is enabled and active                                |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 3.4.4.2 - Configure IPv6 ip6tables                                                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.4.2.1 - Ensure ip6tables loopback traffic is configured                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.4.2.2 - Ensure ip6tables outbound and established connections are configured |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.4.2.3 - Ensure ip6tables firewall rules exist for all open ports             |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.4.2.4 - Ensure ip6tables default deny firewall policy                        |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 3.4.4.2.5 - Ensure ip6tables is enabled and active                               |

| Date       | Version | Changes for this version                                                                                                                                                                                                                          |
|------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.4 - Ensure administrators are notified if an audit processing failure occurs by modifying /etc/aliases""                                                                                                                |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 4.1 - Configure System Accounting (auditd)                                                                                                                                                                                       |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.5 - Ensure the SA and ISSO are notified when the audit storage volume is full                                                                                                                                         |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.6 - Ensure an audit event is generated for any successful/unsuccessful use of the chage" command"                                                                                                                     |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.7 - Ensure the operating system is configured to audit the execution of the fremovexattr" system call"                                                                                                                |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.8 - Ensure the operating system is configured to audit the execution of the fsetxattr" system call"                                                                                                                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.9 - Ensure the operating system is configured to audit the execution of the lsetxattr" system call"                                                                                                                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.10 - Ensure the operating system is configured to audit the execution of the removexattr" system call"                                                                                                                |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.11 - Ensure the operating system is configured to audit the execution of the lremovexattr" system call"                                                                                                               |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.12 - Ensure the operating system generates audit records when successful/unsuccessful attempts to use the su" command by performing the following command to check the file system rules in "/etc/audit/audit.rules"" |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.13 - Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect /etc/sudoers.d/""                                                    |



| Date       | Version | Changes for this version                                                                                                                                                                             |
|------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.14 - Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect /etc/sudoers""          |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.15 - Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect /etc/gshadow""          |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.16 - Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect /etc/security/opasswd"" |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.17 - Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow""           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.19 - Ensure the audit system prevents unauthorized changes                                                                                                               |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.20 - Ensure the operating system takes the appropriate action when the audit storage volume is full                                                                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.21 - Ensure the operating system takes the appropriate action when the audit storage volume is full                                                                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.23 - Ensure the operating system takes the appropriate action when an audit processing failure occurs                                                                    |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.29 - Ensure unsuccessful unauthorized file access attempts are collected                                                                                                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.32 - Ensure use of privileged commands is collected                                                                                                                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.34 - Ensure kernel module loading and unloading is collected                                                                                                             |

| Date       | Version | Changes for this version                                                                                                                                                                   |
|------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.35 - Ensure system administrator actions (sudolog) are collected                                                                                               |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.37 - Ensure the operating system audits the execution of privileged functions                                                                                  |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.41 - Ensure the operating system's audit logs have a mode of 0600" or less permissive"                                                                         |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.42 - Ensure the operating system's audit logs are owned by root""                                                                                              |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.43 - Ensure the audit logs are group-owned by root""                                                                                                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.44 - Ensure the audit log directory is owned by root" to prevent unauthorized read access"                                                                     |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.45 - Ensure the audit log directory is group-owned by root" to prevent unauthorized read access"                                                               |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.46 - Ensure the audit log directories have a mode of 0700" or less permissive by first determining where the audit logs are stored"                            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.47 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the chcon" command"                          |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.48 - Ensure the operating system is configured to audit the execution of the setxattr" system call"                                                            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.49 - Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd"" |

| Date       | Version | Changes for this version                                                                                                                                                                  |
|------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.50 - Ensure the operating system generates audit records for all account creations, modifications, disabling, and termination events that affect /etc/group"" |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.51 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the ssh-agent""                             |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.52 - Ensure an audit event is generated for any successful/unsuccessful use of the passwd" command"                                                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.53 - Ensure an audit event is generated for any successful/unsuccessful use of the mount" command"                                                            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.54 - Ensure an audit event is generated for any successful/unsuccessful use of the umount" command"                                                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.55 - Ensure an audit event is generated for any successful/unsuccessful use of the mount" syscall"                                                            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.56 - Ensure an audit event is generated for any successful/unsuccessful use of the unix_update""                                                              |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.57 - Ensure an audit event is generated for any successful/unsuccessful use of postdrop""                                                                     |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.58 - Ensure an audit event is generated for any successful/unsuccessful use of postqueue""                                                                    |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.59 - Ensure an audit event is generated for any successful/unsuccessful use of semanage""                                                                     |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.60 - Ensure an audit event is generated for any successful/unsuccessful use of setfiles""                                                                     |

| Date       | Version | Changes for this version                                                                                                                                                |
|------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.61 - Ensure an audit event is generated for any successful/unsuccessful use of userhelper""                                                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.62 - Ensure an audit event is generated for any successful/unsuccessful use of setsebool""                                                  |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.63 - Ensure an audit event is generated for any successful/unsuccessful use of unix_chkpwd""                                                |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.64 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the ssh-keysign""         |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.65 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the setfacl" command"     |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.66 - Ensure an audit event is generated for any successful/unsuccessful use of the pam_timestamp_check" command"                            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.67 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the newgrp" command"      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.68 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the init_module" command" |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.69 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the rename" command"      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.70 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the renameat" command"    |

| Date       | Version | Changes for this version                                                                                                                                                  |
|------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.71 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the rmdir" command"         |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.72 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the unlink" command"        |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.73 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the unlinkat" command"      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.74 - Ensure an audit event is generated for any successful/unsuccessful use of the gpasswd" command"                                          |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.75 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the finit_module" command"  |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.76 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the delete_module" command" |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.77 - Ensure an audit event is generated for any successful/unsuccessful use of the crontab" command"                                          |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.78 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the chsh" command"          |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.79 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the truncate" command"      |

| Date       | Version | Changes for this version                                                                                                                                                          |
|------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.80 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the openat" command"                |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.81 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the open" system call"              |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.82 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the open_by_handle_at" system call" |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.83 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the ftruncate" command"             |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.84 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the creat" system call"             |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.85 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the chown" command"                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.86 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the chmod" command"                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.87 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the lchown" system call"            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.88 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the fchownat" system call"          |

| Date       | Version | Changes for this version                                                                                                                                                 |
|------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.89 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the fchown" system call"   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.90 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the fchmod" system call"   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.91 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the fchmodat" system call" |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.92 - Ensure an audit event is generated for any successful/unsuccessful use of the sudo" command"                                            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.93 - Ensure an audit event is generated for any successful/unsuccessful use of the usermod" command"                                         |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.94 - Ensure the operating system generates an audit record when there are successful/unsuccessful attempts to use the chacl" command"        |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.95 - Ensure the operating system is configured to audit the execution of the module management program kmod""                                |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.96 - Ensure the operating system generates an audit record when there are successful/unsuccessful modifications to the faillock" file occur" |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.97 - Ensure the operating system generates an audit record when there are successful/unsuccessful modifications to the lastlog" file"        |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.98 - Ensure the operating system enables auditing of processes that start prior to the audit daemon                                          |

| Date       | Version | Changes for this version                                                                                                                                             |
|------------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.101 - Ensure the files in directory /etc/audit/rules.d/" and the "/etc/audit/auditd.conf" file have a mode of "0640" or less permissive" |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.102 - Ensure the audit tools are protected from unauthorized access, deletion, or modification by checking the permissive mode           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.103 - Ensure the audit tools are owned by root" to prevent any unauthorized access                                                       |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.104 - Ensure the audit tools are group-owned by root" to prevent any unauthorized access                                                 |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 4.1.1 - Ensure auditing is enabled                                                                                                                  |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.1.1 - Ensure auditd is installed                                                                                                         |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.1.2 - Ensure auditd service is enabled                                                                                                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.1.5 - Ensure the audit service is configured to produce audit records                                                                    |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.1.2.5 - Ensure the operating system has the packages required for offloading audit logs                                                    |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 4.2 - Configure Logging                                                                                                                             |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.2.3 - Ensure permissions on all logfiles are configured                                                                                    |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.2.1.3 - Ensure the operating system monitors all remote access methods                                                                     |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.2.1.4 - Ensure rsyslog Service is enabled                                                                                                  |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.2.1.5 - Ensure rsyslog default file permissions configured                                                                                 |



| Date       | Version | Changes for this version                                                                                                 |
|------------|---------|--------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.2.1.6 - Ensure logging is configured                                                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.2.1.8 - Ensure remote rsyslog messages are only accepted on designated log hosts.              |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.2.1.9 - Ensure rsyslog" is configured to log cron events"                                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.2.2.2 - Ensure journald is configured to compress large log files                              |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 4.2.2.3 - Ensure journald is configured to write logfiles to persistent disk                     |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 5 - Access, Authentication and Authorization                                                            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.6 - Ensure root login is restricted to system console                                          |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.9 - Ensure the operating system prevents system daemons from using Kerberos for authentication |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.10 - Ensure the krb5-workstation package has not been installed on the system                  |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.12 - Ensure fapolicyd" is installed"                                                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.17 - Ensure fapolicyd" is enabled and running"                                                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.18 - Ensure fapolicyd" employs a deny-all                                                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.20 - Ensure the operating system has enabled the use of the USBGuard                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.1.1 - Ensure cron daemon is enabled                                                            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.1.8 - Ensure at/cron is restricted to authorized users                                         |

| Date       | Version | Changes for this version                                                                                                                                                             |
|------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 5.2 - SSH Server Configuration                                                                                                                                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.2 - Ensure SSH private key files have a passcode                                                                                                         |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.3 - Ensure SSH access is limited                                                                                                                         |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.6 - Ensure SSH LogLevel is appropriate                                                                                                                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.7 - Ensure SSH X11 forwarding is disabled                                                                                                                |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.8 - Ensure SSH MaxAuthTries is set to 4 or less                                                                                                          |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.9 - Ensure SSH IgnoreRhosts is enabled                                                                                                                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.10 - Ensure SSH HostbasedAuthentication is disabled                                                                                                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.11 - Ensure SSH root login is disabled                                                                                                                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.12 - Ensure SSH PermitEmptyPasswords is disabled                                                                                                         |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.13 - Ensure all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.14 - Ensure SSH PermitUserEnvironment is disabled                                                                                                        |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.15 - Ensure SSH Idle Timeout Interval is configured                                                                                                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.16 - Ensure SSH LoginGraceTime is set to one minute or less                                                                                              |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.17 - Ensure SSH warning banner is configured                                                                                                             |

| Date       | Version | Changes for this version                                                                                                   |
|------------|---------|----------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.18 - Ensure SSH PAM is enabled                                                                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.19 - Ensure SSH AllowTcpForwarding is disabled                                                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.20 - Ensure SSH MaxStartups is configured                                                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.21 - Ensure SSH MaxSessions is set to 4 or less                                                |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.25 - Ensure system-wide crypto policy is not over-ridden                                       |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.26 - Ensure the SSH daemon performs strict mode checking of home directory configuration files |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.27 - Ensure the SSH daemon performs compression after a user successfully authenticates        |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.28 - Ensure the SSH daemon does not allow authentication using known host's authentication     |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.29 - Ensure the SSH daemon does not allow Kerberos authentication                              |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.30 - Ensure null passwords cannot be used                                                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.31 - Ensure SSH provides users with feedback on when account accesses last occurred            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.33 - Ensure the SSH server is configured to force frequent session key renegotiation           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.34 - Ensure the SSH daemon prevents remote hosts from connecting to the proxy display          |

| Date       | Version | Changes for this version                                                                                                                                                             |
|------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.36 - Ensure the SSH daemon does not allow GSSAPI authentication                                                                                          |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.37 - Ensure SSH is installed                                                                                                                             |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.2.38 - Ensure all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.3.1 - Create custom authselect profile                                                                                                                     |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.3.2 - Select authselect profile                                                                                                                            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.3.3 - Ensure authselect includes with-faillock                                                                                                             |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 5.4 - Configure PAM                                                                                                                                                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.1 - Ensure password creation requirements are configured                                                                                                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.2 - Ensure the system locks an account after three unsuccessful logon attempts                                                                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.3 - Ensure the <code>/etc/security/faillock.conf</code> file is configured to lock an account after three unsuccessful logon attempts within 15 minutes" |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.4 - Ensure the system locks an account after three unsuccessful logon attempts within a period of 15 minutes                                             |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.5 - Ensure the <code>/etc/security/faillock.conf</code> file is configured to lock an account after three unsuccessful logon attempts"                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.6 - Ensure lockout for failed password attempts is configured                                                                                            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.7 - Ensure password reuse is limited                                                                                                                     |

| Date       | Version | Changes for this version                                                                                                                                                                               |
|------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.8 - Ensure password hashing algorithm is SHA-512                                                                                                                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.9 - Ensure a minimum number of hash rounds is configured                                                                                                                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.10 - Ensure the system locks an account after three unsuccessful logon attempts within a period of 15 minutes until released by an administrator                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.11 - Ensure the <code>/etc/security/faillock.conf</code> file is configured to lock an account until released by an administrator after three unsuccessful logon attempts" |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.12 - Ensure the faillock directory contents persist after a reboot                                                                                                         |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.13 - Ensure the <code>/etc/security/faillock.conf</code> file is configured to use a non-default faillock directory to ensure contents persist after reboot"               |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.14 - Ensure the system prevents informative messages to the user about logon information                                                                                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.15 - Ensure the <code>/etc/security/faillock.conf</code> file is configured to prevent informative messages about logon attempts"                                          |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.16 - Ensure the system logs user name information when unsuccessful logon attempts occur                                                                                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.17 - Ensure the <code>/etc/security/faillock.conf</code> file is configured to log user name information when unsuccessful logon attempts occur"                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.18 - Ensure the system includes the root account when locking an account after three unsuccessful logon attempts within a period of 15 minutes                             |

| Date       | Version | Changes for this version                                                                                                                                                     |
|------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.19 - Ensure the <code>/etc/security/faillock.conf</code> file is configured to log user name information when unsuccessful logon attempts occur" |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.20 - Ensure the operating system prohibits password reuse for a minimum of five generations                                                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.23 - Ensure the <code>pam_unix.so</code> module is configured to use sha512"                                                                     |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.24 - Ensure the <code>pam_faillock.so</code> module is present in the <code>/etc/pam.d/system-auth</code> file"                                  |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.25 - Ensure blank or null passwords in the <code>system-auth</code> file cannot be used"                                                         |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.26 - Ensure blank or null passwords in the <code>password-auth</code> file cannot be used"                                                       |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.4.27 - Ensure the <code>pam_faillock.so</code> module is present in the <code>/etc/pam.d/password-auth</code> file"                                |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.2 - Ensure system accounts are secured                                                                                                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.3 - Ensure default user shell timeout is 900 seconds or less                                                                                     |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.4 - Ensure the interactive user account passwords are using a strong password hash                                                               |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.5 - Ensure default group for the root account is GID 0                                                                                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.6 - Ensure default user umask is 027 or more restrictive                                                                                         |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 5.5.1 - Set Shadow Password Suite Parameters                                                                                                                |

| Date       | Version | Changes for this version                                                                                                                                                |
|------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.1.1 - Ensure password expiration is 365 days or less                                                                                        |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.1.2 - Ensure the shadow password suite configuration is set to encrypt password with a FIPS 140-2 approved cryptographic hashing algorithm. |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.1.3 - Ensure the value of the maxrepeat" option in "/etc/security/pwquality.conf" is "3"                                                    |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.1.4 - Ensure the value of the difok" option in "/etc/security/pwquality.conf" is "8"                                                        |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.1.5 - Ensure the value of the minclass" option in "/etc/security/pwquality.conf" is "4"                                                     |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.1.6 - Ensure the value of the maxclassrepeat" option in "/etc/security/pwquality.conf" is "4"                                               |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.1.7 - Ensure the value for dcredit" in "/etc/security/pwquality.conf" is "-1"                                                               |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.1.8 - Ensure the value for lcredit" in "/etc/security/pwquality.conf" is "-1"                                                               |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.1.9 - Ensure the value for ucredit" in "/etc/security/pwquality.conf" is "-1"                                                               |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.1.10 - Ensure the operating system uses pwquality" to enforce the password complexity rules"                                                |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.1.11 - Ensure minimum days between password changes is 7 or more                                                                            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.1.12 - Ensure password expiration warning days is 7 or more                                                                                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.1.13 - Ensure inactive password lock is 30 days or less                                                                                     |

| Date       | Version | Changes for this version                                                                                                                                                |
|------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.1.15 - Ensure the minimum time period between password changes for each user account is one day or greater                                  |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.1.16 - Ensure the operating system enforces 24 hours/1 day as the minimum password lifetime for new user accounts                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.1.20 - Ensure the operating system enforces a minimum 15-character password length for new user accounts                                    |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.1.21 - Ensure the value for ocredit" in "/etc/security/pwquality.conf" is "-1""                                                             |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.1.22 - Ensure the operating system prevents the use of dictionary words for passwords                                                       |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 5.5.1.23 - Ensure the operating system enforces a delay of at least four seconds between console logon prompts following a failed logon attempt |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.1 - Audit system file permissions                                                                                                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.10 - Ensure the root account is the only account that has unrestricted access to the operating system                                       |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.11 - Ensure no world writable files exist                                                                                                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.12 - Ensure no unowned files or directories exist                                                                                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.13 - Ensure no ungrouped files or directories exist                                                                                         |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.14 - Ensure all public directories are owned by root or a system account                                                                    |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.15 - Audit SUID executables                                                                                                                 |



| Date       | Version | Changes for this version                                                                                               |
|------------|---------|------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.16 - Audit SGID executables                                                                |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.17 - Ensure the /var/log/messages" file has mode "0640" or less permissive"                |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.18 - Ensure the /var/log/messages" file is owned by root"                                  |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.19 - Ensure the /var/log/messages" file is group-owned by root"                            |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.20 - Ensure the /var/log" directory has a mode of "0755" or less"                          |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.21 - Ensure the /var/log" directory is owned by root"                                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.22 - Ensure the /var/log" directory is group-owned by root"                                |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.23 - Ensure the system commands contained in the /bin                                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.24 - Ensure the system commands contained in the /bin                                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.25 - Ensure the system commands contained in /bin                                          |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.26 - Ensure the system-wide shared library files contained in the /lib                     |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.27 - Ensure the system-wide shared library files are owned by root""                       |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.28 - Ensure the system-wide shared library files are group-owned by root""                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.29 - Ensure world-writable directories are owned by root, sys, bin, or an application user |

| Date       | Version | Changes for this version                                                                                                                                   |
|------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.30 - Ensure world-writable directories are group-owned by root, sys, bin, or an application group                              |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.1.35 - Ensure the operating system initiates a session lock after a 15-minute period of inactivity for graphical user interfaces |
| 11/25/2024 | 2.0.0   | DROPPED SECTION: 6.2 - User and Group Settings                                                                                                             |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.1 - Ensure password fields are not empty                                                                                       |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.2 - Ensure no legacy "+" entries exist in /etc/passwd"                                                                         |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.3 - Ensure root PATH Integrity                                                                                                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.4 - Ensure no legacy "+" entries exist in /etc/shadow"                                                                         |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.5 - Ensure no legacy "+" entries exist in /etc/group"                                                                          |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.7 - Ensure users' home directories permissions are 750 or more restrictive                                                     |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.8 - Ensure emergency accounts have been provisioned with an expiration date of 72 hours                                        |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.9 - Ensure users own their home directories                                                                                    |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.10 - Ensure users' dot files are not group or world writable                                                                   |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.11 - Ensure no users have .forward files                                                                                       |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.12 - Ensure no users have .netrc files                                                                                         |

| Date       | Version | Changes for this version                                                                                                                                                            |
|------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.13 - Ensure users' .netrc Files are not group or world accessible                                                                                       |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.14 - Ensure no users have .rhosts files                                                                                                                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.21 - Ensure all users' home directories exist                                                                                                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.22 - Ensure the assigned home directory of all local interactive users is group-owned by that user's primary GID                                        |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.23 - Ensure the assigned home directory of all local interactive users exists                                                                           |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.25 - Ensure all local initialization files have a mode of 0740" or less permissive"                                                                     |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.26 - Ensure all local files and directories have a valid owner                                                                                          |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.27 - Ensure all local files and directories have a valid group                                                                                          |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.30 - Ensure local interactive users have a home directory assigned                                                                                      |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.31 - Ensure the operating system limits the number of concurrent sessions to 10" for all accounts and/or account types"                                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.34 - Ensure the operating system prevents a user from overriding settings for graphical user interfaces                                                 |
| 11/25/2024 | 2.0.0   | DROPPED RECOMMENDATION: 6.2.35 - Ensure all files and directories contained in a local interactive user home directory, excluding local initialization files, have a mode of 0750"" |

#### MOVED ITEMS:

|            |       |                                                                                          |
|------------|-------|------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0 | MOVED RECOMMENDATION: 1.9 - Ensure the tmux" package installed moved from 1.32 in 1.0.0" |
|------------|-------|------------------------------------------------------------------------------------------|

| Date       | Version | Changes for this version                                                                                                                                                 |
|------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1 - Ensure the system has the packages required to enable the hardware random number generator entropy gatherer service moved from 1.31 in 1.0.0 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.12 - Ensure the operating system accepts PIV credentials moved from 1.22 in 1.0.0                                                                |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.13 - Ensure the operating system has the packages required for multifactor authentication moved from 1.20 in 1.0.0                               |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.1.11 - Ensure the operating system disables the ability to load the firewire-core kernel module moved from 1.28 in 1.0.0                       |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.1.12 - Ensure a camera is not installed moved from 2.2.24 in 1.0.0                                                                             |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.12 - Ensure all non-root local partitions are mounted with the nodev" option moved from 1.1.26 in 1.0.0"                                     |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.1.2 - Ensure nodev option set on /tmp partition moved from 1.1.3 in 1.0.0                                                                    |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.1.3 - Ensure nosuid option set on /tmp partition moved from 1.1.4 in 1.0.0                                                                   |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.1.4 - Ensure noexec option set on /tmp partition moved from 1.1.5 in 1.0.0                                                                   |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.2.2 - Ensure nodev option set on /dev/shm partition moved from 1.1.15 in 1.0.0                                                               |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.2.3 - Ensure nosuid option set on /dev/shm partition moved from 1.1.16 in 1.0.0                                                              |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.2.4 - Ensure noexec option set on /dev/shm partition moved from 1.1.17 in 1.0.0                                                              |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.3.1 - Ensure separate partition exists for /home moved from 1.1.13 in 1.0.0                                                                  |

| Date       | Version | Changes for this version                                                                                                                                                         |
|------------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.3.2 - Ensure nodev option set on /home partition moved from 1.1.14 in 1.0.0                                                                          |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.3.4 - Ensure a separate file system/partition has been created for non-privileged local interactive user home directories moved from 1.1.30 in 1.0.0 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.3.6 - Ensure file systems that contain user home directories are mounted with the noexec" option moved from 1.1.38 in 1.0.0"                         |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.4.1 - Ensure separate partition exists for /var moved from 1.1.6 in 1.0.0                                                                            |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.5.1 - Ensure separate partition exists for /var/tmp moved from 1.1.7 in 1.0.0                                                                        |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.5.2 - Ensure nodev option set on /var/tmp partition moved from 1.1.8 in 1.0.0                                                                        |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.5.3 - Ensure nosuid option set on /var/tmp partition moved from 1.1.9 in 1.0.0                                                                       |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.5.4 - Ensure noexec option set on /var/tmp partition moved from 1.1.10 in 1.0.0                                                                      |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.6.1 - Ensure separate partition exists for /var/log moved from 1.1.11 in 1.0.0                                                                       |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.7.1 - Ensure separate partition exists for /var/log/audit moved from 1.1.12 in 1.0.0                                                                 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.8.1 - Ensure the /boot" directory is mounted with the "nosuid" option moved from 1.1.25 in 1.0.0"                                                    |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.9.1 - Ensure the /boot/efi" directory is mounted with the "nosuid" option moved from 1.1.37 in 1.0.0"                                                |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.10.1 - Ensure file systems that are being NFS-imported are mounted with the nodev" option moved from 1.1.27 in 1.0.0"                                |

| Date       | Version | Changes for this version                                                                                                                                       |
|------------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.10.2 - Ensure file systems being imported via NFS are mounted with the nosuid" option moved from 1.1.29 in 1.0.0"                  |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.10.3 - Ensure file systems being imported via NFS are mounted with the noexec" option moved from 1.1.28 in 1.0.0"                  |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.11.1 - Ensure nodev option set on removable media partitions moved from 1.1.18 in 1.0.0                                            |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.11.2 - Ensure nosuid option set on removable media partitions moved from 1.1.19 in 1.0.0                                           |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.1.2.11.3 - Ensure noexec option set on removable media partitions moved from 1.1.20 in 1.0.0                                           |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.2.1.1 - Ensure GPG keys are configured moved from 1.2.1 in 1.0.0                                                                       |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.2.1.2 - Ensure gpgcheck is globally activated moved from 1.2.2 in 1.0.0                                                                |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.2.1.4 - Ensure package manager repositories are configured moved from 1.2.3 in 1.0.0                                                   |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.2.1.5 - Ensure DNF is configured to perform a signature check on local packages moved from 1.2.4 in 1.0.0                              |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.2.2.1 - Ensure updates, patches, and additional security software are installed moved from 1.10 in 1.0.0                               |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.2.2.4 - Ensure the operating system removes all software components after updated versions have been installed moved from 6.3 in 1.0.0 |
| 11/25/2024 | 2.0.0   | MOVED SECTION: 1.3 - Mandatory Access Control moved from 1.7 in 1.0.0                                                                                          |

| Date       | Version | Changes for this version                                                                                                                                                                   |
|------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | MOVED SECTION: 1.3.1 - Configure SELinux moved from 1.7.1 in 1.0.0                                                                                                                         |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.3.1.1 - Ensure SELinux is installed moved from 1.7.1.1 in 1.0.0                                                                                                    |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.3.1.2 - Ensure SELinux is not disabled in bootloader configuration moved from 1.7.1.2 in 1.0.0                                                                     |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.3.1.3 - Ensure SELinux policy is configured moved from 1.7.1.3 in 1.0.0                                                                                            |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.3.1.6 - Ensure no unconfined services exist moved from 1.7.1.5 in 1.0.0                                                                                            |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.3.1.7 - Ensure the MCS Translation Service (mcstrans) is not installed moved from 1.7.1.7 in 1.0.0                                                                 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.3.1.8 - Ensure the operating system has the polycoreutils package installed moved from 1.7.1.8 in 1.0.0                                                            |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.3.1.9 - Ensure SETroubleshoot is not installed moved from 1.7.1.6 in 1.0.0                                                                                         |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.4.1 - Ensure bootloader password is set moved from 1.5.2 in 1.0.0                                                                                                  |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.4.3 - Ensure the operating system requires authentication for rescue mode moved from 1.5.6 in 1.0.0                                                                |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.4.4 - Ensure the operating system requires authentication upon booting into emergency mode moved from 1.5.15 in 1.0.0                                              |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.4.7 - Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed seven times within two seconds moved from 1.5.12 in 1.0.0 |

| Date       | Version | Changes for this version                                                                                                                                                |
|------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.4.8 - Ensure GRUB 2 is configured to enable page poisoning to mitigate use-after-free vulnerabilities moved from 1.5.7 in 1.0.0                 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.4.9 - Ensure GRUB 2 is configured to enable poisoning of SLUB/SLAB objects to mitigate use-after-free vulnerabilities moved from 1.5.9 in 1.0.0 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.4.10 - Ensure GRUB 2 is configured to disable vsyscalls moved from 1.5.8 in 1.0.0                                                               |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.5.7 - Ensure kernel core dumps are disabled unless needed moved from 1.6.5 in 1.0.0                                                             |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.5.8 - Ensure the operating system enables hardening for the BPF JIT moved from 1.33 in 1.0.0                                                    |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.5.9 - Ensure kernel page-table isolation is enabled moved from 1.24 in 1.0.0                                                                    |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.5.10 - Ensure the NX (no-execution) bit flag is set on the system moved from 1.23 in 1.0.0                                                      |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.5.11 - Ensure the operating system disables the use of user namespaces moved from 1.30 in 1.0.0                                                 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.5.12 - Ensure kernel image loading is disabled moved from 1.15 in 1.0.0                                                                         |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.5.13 - Ensure the operating system is configured to enable DAC on symlinks moved from 1.16 in 1.0.0                                             |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.5.14 - Ensure the operating system is configured to boot to the command line moved from 1.5.10 in 1.0.0                                         |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.5.15 - Ensure the operating system is configured to enable DAC on hardlinks moved from 1.17 in 1.0.0                                            |



| Date       | Version | Changes for this version                                                                                                                                                    |
|------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.5.16 - Ensure the operating system restricts exposed kernel pointer addresses access moved from 1.27 in 1.0.0                                       |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.5.17 - Ensure the operating system is configured to restrict access to the kernel message buffer moved from 1.18 in 1.0.0                           |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.5.18 - Ensure the operating system disables core dumps for all users moved from 1.6.6 in 1.0.0                                                      |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.5.19 - Ensure the operating system is configured to prevent kernel profiling by unprivileged users moved from 1.19 in 1.0.0                         |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.5.20 - Ensure the operating system restricts usage of ptrace to descendant processes moved from 1.26 in 1.0.0                                       |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.5.21 - Ensure the operating system prevents privilege escalation through the kernel by disabling access to the bpf syscall moved from 1.25 in 1.0.0 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.5.22 - Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed moved from 1.5.11 in 1.0.0                |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.5.23 - Ensure the operating system implements the Endpoint Security for Linux Threat Prevention tool moved from 1.34 in 1.0.0                       |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.6.9 - Ensure PKI-based authentication has valid certificates moved from 5.7 in 1.0.0                                                                |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.6.10 - Ensure system-wide crypto policies are in effect moved from 5.2.35 in 1.0.0                                                                  |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.6.11 - Ensure the operating system implements certificate status checking for multifactor authentication moved from 1.21 in 1.0.0                   |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.6.12 - Ensure the OpenSSL library is configured to use only ciphers employing FIPS 140-2-approved algorithms moved from 5.14 in 1.0.0               |

| Date       | Version | Changes for this version                                                                                                                                                                                                       |
|------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.6.13 - Ensure the OpenSSL library is configured to use only DoD-approved TLS encryption moved from 5.15 in 1.0.0                                                                                       |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.6.14 - Ensure the GnuTLS library is configured to only allow DoD-approved SSL/TLS Versions moved from 5.16 in 1.0.0                                                                                    |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.7.1 - Ensure message of the day is configured properly moved from 1.8.2 in 1.0.0                                                                                                                       |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.7.2 - Ensure local login warning banner is configured properly moved from 1.8.3 in 1.0.0                                                                                                               |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.7.3 - Ensure remote login warning banner is configured properly moved from 1.8.4 in 1.0.0                                                                                                              |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.7.7 - Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a command line user logon moved from 1.8.1 in 1.0.0 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.8.1 - Ensure GNOME Display Manager is removed moved from 1.9.2 in 1.0.0                                                                                                                                |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.8.2 - Ensure GDM login banner is configured moved from 1.9.3 in 1.0.0                                                                                                                                  |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.8.8 - Ensure the operating system does not allow an unattended or automatic logon to the system via a graphical user interface moved from 1.9.7 in 1.0.0                                               |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.8.10 - Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed when using a graphical user interface moved from 1.9.8 in 1.0.0                              |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.8.12 - Ensure the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated moved from 1.9.9 in 1.0.0                                                |

| Date       | Version | Changes for this version                                                                                                                                                                   |
|------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.8.14 - Ensure the operating system disables the user logon list for graphical user interfaces moved from 1.9.10 in 1.0.0                                           |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.8.16 - Ensure the operating system prevents users from overriding the session idle-delay setting for the graphical user interface moved from 1.9.11 in 1.0.0       |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.8.17 - Ensure the operating system prevents users from overriding the screensaver lock-enabled setting for the graphical user interface moved from 1.9.12 in 1.0.0 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.8.19 - Ensure the operating system enables a user's session lock until that user re-establishes access moved from 6.1.34 in 1.0.0                                  |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 1.8.19 - Ensure the operating system enables a user's session lock until that user re-establishes access moved from 6.2.32 in 1.0.0                                  |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.1.22 - Ensure automated bug reporting tools are not installed moved from 2.2.21 in 1.0.0                                                                           |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.1.24 - Ensure the sendmail package is not installed moved from 2.2.22 in 1.0.0                                                                                     |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.1.25 - Ensure the rsh-server package is not installed moved from 2.2.23 in 1.0.0                                                                                   |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.1.27 - Ensure the operating system is configured to mask the debug-shell systemd service moved from 2.2.25 in 1.0.0                                                |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.1.28 - Ensure the gssproxy package has not been installed on the system moved from 2.2.30 in 1.0.0                                                                 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.1.29 - Ensure the iprutils package has not been installed on the system moved from 2.2.31 in 1.0.0                                                                 |

| Date       | Version | Changes for this version                                                                                                                                                                  |
|------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.1.30 - Ensure the krb5-server package has not been installed on the system moved from 2.2.33 in 1.0.0                                                             |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.1.31 - Ensure a TFTP server has not been installed on the system moved from 2.2.26 in 1.0.0                                                                       |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.1.32 - Ensure the tuned package has not been installed on the system moved from 2.2.32 in 1.0.0                                                                   |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.1.33 - Ensure the operating system has enabled the hardware random number generator entropy gatherer service moved from 2.2.20 in 1.0.0                           |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.1.34 - Ensure the operating system is configured to prevent unrestricted mail relaying moved from 2.2.27 in 1.0.0                                                 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.1.35 - Ensure the TFTP daemon is configured to operate in secure mode moved from 2.2.28 in 1.0.0                                                                  |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.2.4 - Ensure telnet client is not installed moved from 2.3.2 in 1.0.0                                                                                             |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.3.1 - Ensure time synchronization is in use moved from 2.2.1.1 in 1.0.0                                                                                           |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.3.2 - Ensure chrony is configured moved from 2.2.1.2 in 1.0.0                                                                                                     |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.3.4 - Ensure the operating system is securely comparing internal information system clocks at least every 24 hours with an NTP server moved from 2.2.1.3 in 1.0.0 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.3.5 - Ensure the operating system disables network management of the chrony daemon moved from 2.2.1.5 in 1.0.0                                                    |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.3.6 - Ensure the operating system disables the chrony daemon from acting as a server moved from 2.2.1.4 in 1.0.0                                                  |

| Date       | Version | Changes for this version                                                                                                                 |
|------------|---------|------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | MOVED SECTION: 2.4.1 - Configure cron moved from 5.1 in 1.0.0                                                                            |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.4.1.2 - Ensure permissions on /etc/crontab are configured moved from 5.1.2 in 1.0.0                              |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.4.1.3 - Ensure permissions on /etc/cron.hourly are configured moved from 5.1.3 in 1.0.0                          |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.4.1.4 - Ensure permissions on /etc/cron.daily are configured moved from 5.1.4 in 1.0.0                           |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.4.1.5 - Ensure permissions on /etc/cron.weekly are configured moved from 5.1.5 in 1.0.0                          |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.4.1.6 - Ensure permissions on /etc/cron.monthly are configured moved from 5.1.6 in 1.0.0                         |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.4.1.7 - Ensure permissions on /etc/cron.d are configured moved from 5.1.7 in 1.0.0                               |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.5.1 - Ensure USBGuard is installed on the operating system moved from 5.19 in 1.0.0                              |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.5.2 - Ensure USBGuard has a policy configured moved from 5.13 in 1.0.0                                           |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 2.5.3 - Ensure the operating system enables Linux audit logging of the USBGuard daemon moved from 4.1.100 in 1.0.0 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 3.4 - Ensure at least two name servers are configured if using DNS resolution moved from 3.7 in 1.0.0              |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 3.1.2 - Ensure wireless interfaces are disabled moved from 3.5 in 1.0.0                                            |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 3.1.4 - Ensure network interfaces are not in promiscuous mode moved from 3.2.14 in 1.0.0                           |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 3.3.2 - Ensure packet redirect sending is disabled moved from 3.1.2 in 1.0.0                                       |

| Date       | Version | Changes for this version                                                                                                                                            |
|------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 3.3.8 - Ensure source routed packets are not accepted moved from 3.2.1 in 1.0.0                                                               |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 3.3.9 - Ensure suspicious packets are logged moved from 3.2.4 in 1.0.0                                                                        |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 4.1.2 - Ensure the firewall is configured to remove unnecessary use of functions, ports, protocols, and/or services moved from 3.4.5 in 1.0.0 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 4.1.3 - Ensure firewalld service is enabled and running moved from 3.4.2.1 in 1.0.0                                                           |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 4.1.6 - Ensure nftables" is configured to allow rate limits on any connection to the system moved from 3.4.3.9 in 1.0.0"                      |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 4.1.7 - Ensure firewalld" is installed moved from 3.4.2.8 in 1.0.0"                                                                           |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 4.1.8 - Ensure firewalld" is configured to employ a deny-all                                                                                  |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 4.1.1.1 - Ensure nftables base chains exist moved from 3.4.3.3 in 1.0.0                                                                       |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 4.1.1.3 - Ensure firewalld drops unnecessary services and ports moved from 3.4.2.6 in 1.0.0                                                   |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 4.1.1.5 - Ensure nftables default deny firewall policy moved from 3.4.3.6 in 1.0.0                                                            |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.1.2 - Ensure permissions on /etc/ssh/sshd_config are configured moved from 5.2.1 in 1.0.0                                                   |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.1.3 - Ensure permissions on SSH private host key files are configured moved from 5.2.4 in 1.0.0                                             |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.1.4 - Ensure permissions on SSH public host key files are configured moved from 5.2.5 in 1.0.0                                              |

| Date       | Version | Changes for this version                                                                                                                                              |
|------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.1.28 - Ensure the SSH server is configured to use only MACs employing FIPS 140-2-approved algorithms moved from 5.2.22 in 1.0.0               |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.1.29 - Ensure the SSH server is configured to use only ciphers employing FIPS 140-2-approved algorithms moved from 5.2.23 in 1.0.0            |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.1.31 - Ensure the SSH server uses strong entropy moved from 5.2.24 in 1.0.0                                                                   |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.1.39 - Ensure SSH is loaded and active moved from 5.2.32 in 1.0.0                                                                             |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.2.1 - Ensure sudo is installed moved from 1.3.1 in 1.0.0                                                                                      |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.2.3 - Ensure sudo commands use pty moved from 1.3.2 in 1.0.0                                                                                  |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.2.4 - Ensure sudo log file exists moved from 1.3.3 in 1.0.0                                                                                   |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.2.8 - Ensure the sudoers security policy is configured to use the invoking user's password for privilege escalation moved from 1.3.7 in 1.0.0 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.2.10 - Ensure access to the su command is restricted moved from 5.8 in 1.0.0                                                                  |
| 11/25/2024 | 2.0.0   | MOVED SECTION: 5.3.2 - Configure authselect moved from 5.3 in 1.0.0                                                                                                   |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.3.3.2.8 - Ensure the operating system enforces a minimum 15-character password length moved from 5.5.1.19 in 1.0.0                            |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.3.3.5.1 - Ensure the date and time of the last successful account logon upon logon is displayed moved from 5.4.22 in 1.0.0                    |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.3.3.6.1 - Ensure the operating system uses multifactor authentication for local access to accounts moved from 5.4.21 in 1.0.0                 |

| Date       | Version | Changes for this version                                                                                                                                                                                            |
|------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.3.3.6.2 - Ensure SSSD prohibits the use of cached authentications after one day moved from 5.11 in 1.0.0                                                                                    |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.3.3.6.3 - Ensure the certificate of the user or group is mapped to the corresponding user or group in the sssd.conf" file moved from 6.2.28 in 1.0.0"                                       |
| 11/25/2024 | 2.0.0   | MOVED SECTION: 5.4 - User Accounts and Environment moved from 5.5 in 1.0.0                                                                                                                                          |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.4.1.6 - Ensure all users last password change date is in the past moved from 5.5.1.14 in 1.0.0                                                                                              |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.4.1.10 - Ensure temporary accounts have been provisioned with an expiration date of 72 hours moved from 6.2.37 in 1.0.0                                                                     |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.4.1.13 - Ensure the maximum time period for existing passwords is restricted to 60 days moved from 5.5.1.18 in 1.0.0                                                                        |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.4.2.1 - Ensure root is the only UID 0 account moved from 6.2.6 in 1.0.0                                                                                                                     |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.4.2.9 - Ensure all accounts on the system are assigned to an active system, application, or user account moved from 6.1.37 in 1.0.0                                                         |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.4.3.4 - Ensure emergency accounts have been provisioned with an expiration date of 72 hours moved from 5.5.8 in 1.0.0                                                                       |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.4.3.5 - Ensure the account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity moved from 5.5.7 in 1.0.0                                         |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.4.3.6 - Ensure the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files moved from 5.5.11 in 1.0.0 |



| Date       | Version | Changes for this version                                                                                                                                                                 |
|------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.4.3.7 - Ensure the operating system enforces a 60-day maximum password lifetime for new user accounts moved from 5.5.1.17 in 1.0.0                               |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.4.3.8 - Ensure the umask default for installed shells is 077" moved from 5.5.10 in 1.0.0"                                                                        |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.4.3.9 - Ensure the default umask for all local interactive users is 077" moved from 5.5.9 in 1.0.0"                                                              |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.4.3.10 - Ensure the operating system initiates a session lock after 15 minutes of inactivity moved from 6.1.36 in 1.0.0                                          |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.4.3.11 - Ensure the operating system prevents users from disabling the tmux terminal multiplexer moved from 6.1.33 in 1.0.0                                      |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.4.3.12 - Ensure the operating system's shell initialization file is configured to start each shell with the tmux terminal multiplexer moved from 6.1.32 in 1.0.0 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.4.3.13 - Ensure the operating system enables the user to initiate a session lock moved from 6.2.33 in 1.0.0                                                      |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 5.4.3.15 - Ensure all local interactive users are assigned a home directory upon creation moved from 6.2.24 in 1.0.0                                               |
| 11/25/2024 | 2.0.0   | MOVED SECTION: 6 - Logging and Auditing moved from 4 in 1.0.0                                                                                                                            |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.1.1 - Ensure AIDE is installed moved from 1.4.1 in 1.0.0                                                                                                         |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.1.2 - Ensure filesystem integrity is regularly checked moved from 1.4.2 in 1.0.0                                                                                 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.1.5 - Ensure the file integrity tool is configured to verify ACLs moved from 1.4.5 in 1.0.0                                                                      |

| Date       | Version | Changes for this version                                                                                                                                                                  |
|------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.1.6 - Ensure the file integrity tool is configured to verify extended attributes moved from 1.4.4 in 1.0.0                                                        |
| 11/25/2024 | 2.0.0   | MOVED SECTION: 6.2.1 - Configure journald moved from 4.2.2 in 1.0.0                                                                                                                       |
| 11/25/2024 | 2.0.0   | MOVED SECTION: 6.2.2 - Configure rsyslog moved from 4.2.1 in 1.0.0                                                                                                                        |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.2.2.1 - Ensure rsyslog is installed moved from 4.2.1.1 in 1.0.0                                                                                                   |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.2.2.4 - Ensure journald is configured to send logs to rsyslog moved from 4.2.2.1 in 1.0.0                                                                         |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.2.2.7 - Ensure rsyslog is configured to send logs to a remote log host moved from 4.2.1.7 in 1.0.0                                                                |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.2.2.9 - Ensure logrotate is configured moved from 4.3 in 1.0.0                                                                                                    |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.2.2.11 - Ensure the rsyslog service is enabled and active moved from 4.2.1.2 in 1.0.0                                                                             |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.2.2.12 - Ensure the operating system has the packages required for encrypting offloaded audit logs moved from 4.1.2.6 in 1.0.0                                    |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.2.2.13 - Ensure the the operating system authenticates the remote logging server for off-loading audit logs moved from 4.1.2.10 in 1.0.0                          |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.2.2.14 - Ensure the operating system encrypts audit records off-loaded onto a different system or media from the system being audited moved from 4.1.2.9 in 1.0.0 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.2.2.15 - Ensure the audit system off-loads audit records onto a different system or media from the system being audited moved from 4.1.2.7 in 1.0.0               |

| Date       | Version | Changes for this version                                                                                                                                                                    |
|------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.1.2 - Ensure auditing for processes that start prior to auditd is enabled moved from 4.1.1.3 in 1.0.0                                                             |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.1.3 - Ensure audit_backlog_limit is sufficient moved from 4.1.1.4 in 1.0.0                                                                                        |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.1.5 - Ensure the operating system allocates a sufficient audit_backlog_limit to capture processes that start prior to the audit daemon moved from 4.1.99 in 1.0.0 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.1.6 - Ensure the operating system's audit daemon is configured to include local events moved from 4.1.38 in 1.0.0                                                 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.1.7 - Ensure the operating system's audit daemon is configured to label all off-loaded audit logs moved from 4.1.39 in 1.0.0                                      |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.1.8 - Ensure the operating system's audit daemon is configured to resolve audit information before writing to disk moved from 4.1.40 in 1.0.0                     |
| 11/25/2024 | 2.0.0   | MOVED SECTION: 6.3.2 - Configure Data Retention moved from 4.1.2 in 1.0.0                                                                                                                   |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.2.1 - Ensure audit log storage size is configured moved from 4.1.2.1 in 1.0.0                                                                                     |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.2.2 - Ensure audit logs are not automatically deleted moved from 4.1.2.2 in 1.0.0                                                                                 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.2.3 - Ensure system is disabled when audit logs are full moved from 4.1.2.3 in 1.0.0                                                                              |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.2.5 - Ensure the operating system allocates audit record storage capacity moved from 4.1.2.4 in 1.0.0                                                             |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.2.6 - Ensure the SA and ISSO are notified in the event of an audit processing failure moved from 4.1.4 in 1.0.0                                                   |

| Date       | Version | Changes for this version                                                                                                                                                                                                    |
|------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.2.7 - Ensure the operating system notifies the SA and ISSO when allocated audit record storage volume reaches 75 percent moved from 4.1.105 in 1.0.0                                              |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.2.8 - Ensure the operating system takes action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity moved from 4.1.2.11 in 1.0.0 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.2.9 - Ensure the audit system is configured to take an appropriate action when the internal event queue is full moved from 4.1.2.8 in 1.0.0                                                       |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.3.1 - Ensure changes to system administration scope (sudoers) is collected moved from 4.1.3 in 1.0.0                                                                                              |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.3.4 - Ensure events that modify date and time information are collected moved from 4.1.25 in 1.0.0                                                                                                |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.3.5 - Ensure events that modify the system's network environment are collected moved from 4.1.27 in 1.0.0                                                                                         |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.3.8 - Ensure events that modify user/group information are collected moved from 4.1.30 in 1.0.0                                                                                                   |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.3.9 - Ensure discretionary access control permission modification events are collected moved from 4.1.28 in 1.0.0                                                                                 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.3.10 - Ensure successful file system mounts are collected moved from 4.1.31 in 1.0.0                                                                                                              |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.3.11 - Ensure session initiation information is collected moved from 4.1.24 in 1.0.0                                                                                                              |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.3.12 - Ensure login and logout events are collected moved from 4.1.22 in 1.0.0                                                                                                                    |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.3.13 - Ensure file deletion events by users are collected moved from 4.1.33 in 1.0.0                                                                                                              |

| Date       | Version | Changes for this version                                                                                                                   |
|------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.3.14 - Ensure events that modify the system's Mandatory Access Controls are collected moved from 4.1.26 in 1.0.0 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.3.20 - Ensure the audit configuration is immutable moved from 4.1.36 in 1.0.0                                    |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 6.3.3.43 - Ensure the audit system prevents unauthorized changes to logon UIDs moved from 4.1.18 in 1.0.0            |
| 11/25/2024 | 2.0.0   | MOVED SECTION: 7 - System Maintenance moved from 6 in 1.0.0                                                                                |
| 11/25/2024 | 2.0.0   | MOVED SECTION: 7.1 - System File Permissions moved from 6.1 in 1.0.0                                                                       |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 7.1.1 - Ensure permissions on /etc/passwd are configured moved from 6.1.2 in 1.0.0                                   |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 7.1.2 - Ensure permissions on /etc/passwd- are configured moved from 6.1.3 in 1.0.0                                  |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 7.1.3 - Ensure permissions on /etc/group are configured moved from 6.1.8 in 1.0.0                                    |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 7.1.4 - Ensure permissions on /etc/group- are configured moved from 6.1.9 in 1.0.0                                   |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 7.1.5 - Ensure permissions on /etc/shadow are configured moved from 6.1.4 in 1.0.0                                   |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 7.1.6 - Ensure permissions on /etc/shadow- are configured moved from 6.1.5 in 1.0.0                                  |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 7.1.7 - Ensure permissions on /etc/gshadow are configured moved from 6.1.6 in 1.0.0                                  |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 7.1.8 - Ensure permissions on /etc/gshadow- are configured moved from 6.1.7 in 1.0.0                                 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 7.1.14 - Ensure there are no .shosts" files on the operating system moved from 6.4 in 1.0.0"                         |

| Date       | Version | Changes for this version                                                                                                                                                                        |
|------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 7.1.15 - Ensure there are no shosts.equiv" files on the operating system moved from 6.5 in 1.0.0"                                                                         |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 7.1.21 - Ensure local initialization files do not execute world-writable programs moved from 6.1.31 in 1.0.0                                                              |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 7.2.3 - Ensure all groups in /etc/passwd exist in /etc/group moved from 6.2.15 in 1.0.0                                                                                   |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 7.2.4 - Ensure shadow group is empty moved from 6.2.20 in 1.0.0                                                                                                           |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 7.2.5 - Ensure no duplicate UIDs exist moved from 6.2.16 in 1.0.0                                                                                                         |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 7.2.6 - Ensure no duplicate GIDs exist moved from 6.2.17 in 1.0.0                                                                                                         |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 7.2.7 - Ensure no duplicate user names exist moved from 6.2.18 in 1.0.0                                                                                                   |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 7.2.8 - Ensure no duplicate group names exist moved from 6.2.19 in 1.0.0                                                                                                  |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 7.2.11 - Ensure all files and directories in the local interactive user home directory are group-owned by a group that the user is a member of moved from 6.2.36 in 1.0.0 |
| 11/25/2024 | 2.0.0   | MOVED RECOMMENDATION: 7.2.15 - Ensure file executable search path statements do not share sensitive home directory information moved from 6.2.29 in 1.0.0                                       |

#### UPDATED ITEMS:

|            |       |                                                                                                                                                                                         |
|------------|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0 | UPDATED RECOMMENDATION: 1.1.1.11 - Ensure the operating system disables the ability to load the firewire-core kernel module - Sections Modified: Remediation Procedure; Audit Procedure |
| 11/25/2024 | 2.0.0 | UPDATED RECOMMENDATION: 1.1.1.12 - Ensure a camera is not installed - Sections Modified: Assessment Status; Remediation Procedure; Audit Procedure                                      |

| Date       | Version | Changes for this version                                                                                                                                                                          |
|------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.1.2.1.2 - Ensure nodev option set on /tmp partition - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure                                    |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.1.2.1.3 - Ensure nosuid option set on /tmp partition - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure                                   |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.1.2.1.4 - Ensure noexec option set on /tmp partition - Sections Modified: Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure                 |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.1.2.2.2 - Ensure nodev option set on /dev/shm partition - Sections Modified: Remediation Procedure; Audit Procedure                                                     |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.1.2.2.3 - Ensure nosuid option set on /dev/shm partition - Sections Modified: Remediation Procedure; Audit Procedure                                                    |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.1.2.2.4 - Ensure noexec option set on /dev/shm partition - Sections Modified: Remediation Procedure; Audit Procedure                                                    |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.1.2.3.1 - Ensure separate partition exists for /home - Sections Modified: Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure                 |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.1.2.3.2 - Ensure nodev option set on /home partition - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure                                   |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.1.2.4.1 - Ensure separate partition exists for /var - Sections Modified: Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure                  |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.1.2.5.1 - Ensure separate partition exists for /var/tmp - Sections Modified: Description; Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure |

| Date       | Version | Changes for this version                                                                                                                                                                                |
|------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.1.2.5.2 - Ensure nodev option set on /var/tmp partition - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure                                      |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.1.2.5.3 - Ensure nosuid option set on /var/tmp partition - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure                                     |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.1.2.5.4 - Ensure noexec option set on /var/tmp partition - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure                                     |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.1.2.6.1 - Ensure separate partition exists for /var/log - Sections Modified: Description; Rationale Statement; Audit Procedure                                                |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.1.2.7.1 - Ensure separate partition exists for /var/log/audit - Sections Modified: Description; Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.1.2.11.1 - Ensure nodev option set on removable media partitions - Sections Modified: Audit Procedure                                                                         |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.1.2.11.2 - Ensure nosuid option set on removable media partitions - Sections Modified: Audit Procedure                                                                        |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.1.2.11.3 - Ensure noexec option set on removable media partitions - Sections Modified: Audit Procedure                                                                        |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.2.1.1 - Ensure GPG keys are configured - Sections Modified: Description; Rationale Statement; Audit Procedure                                                                 |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.2.1.2 - Ensure gpgcheck is globally activated - Sections Modified: Description; Remediation Procedure; Audit Procedure                                                        |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.2.1.4 - Ensure package manager repositories are configured - Sections Modified: Description; Rationale Statement; Audit Procedure                                             |



| Date       | Version | Changes for this version                                                                                                                                                            |
|------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.2.2.1 - Ensure updates, patches, and additional security software are installed - Sections Modified: Profile; Remediation Procedure; Audit Procedure      |
| 11/25/2024 | 2.0.0   | UPDATED SECTION: 1.3.1 - Configure SELinux - Sections Modified: Description                                                                                                         |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.3.1.1 - Ensure SELinux is installed - Sections Modified: Profile                                                                                          |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.3.1.2 - Ensure SELinux is not disabled in bootloader configuration - Sections Modified: Profile; Impact Statement; Remediation Procedure; Audit Procedure |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.3.1.3 - Ensure SELinux policy is configured - Sections Modified: Profile                                                                                  |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.3.1.6 - Ensure no unconfined services exist - Sections Modified: Assessment Status; Impact Statement; Remediation Procedure; Audit Procedure              |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.3.1.7 - Ensure the MCS Translation Service (mcstrans) is not installed - Sections Modified: Profile; Audit Procedure                                      |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.3.1.9 - Ensure SETroubleshoot is not installed - Sections Modified: Profile                                                                               |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.4.1 - Ensure bootloader password is set - Sections Modified: Profile; Description; Impact Statement; Remediation Procedure; Audit Procedure               |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.4.3 - Ensure the operating system requires authentication for rescue mode - Sections Modified: Description; Remediation Procedure; Audit Procedure        |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.4.8 - Ensure GRUB 2 is configured to enable page poisoning to mitigate use-after-free vulnerabilities - Sections Modified: Audit Procedure                |

| Date       | Version | Changes for this version                                                                                                                                                                    |
|------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.4.10 - Ensure GRUB 2 is configured to disable vsyscalls - Sections Modified: Audit Procedure                                                                      |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.5.8 - Ensure the operating system enables hardening for the BPF JIT - Sections Modified: Remediation Procedure; Audit Procedure                                   |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.5.10 - Ensure the NX (no-execution) bit flag is set on the system - Sections Modified: Audit Procedure                                                            |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.5.11 - Ensure the operating system disables the use of user namespaces - Sections Modified: Description; Impact Statement; Remediation Procedure; Audit Procedure |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.5.12 - Ensure kernel image loading is disabled - Sections Modified: Remediation Procedure; Audit Procedure                                                        |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.5.13 - Ensure the operating system is configured to enable DAC on symlinks - Sections Modified: Remediation Procedure; Audit Procedure                            |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.5.14 - Ensure the operating system is configured to boot to the command line - Sections Modified: Assessment Status; Remediation Procedure; Audit Procedure       |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.5.15 - Ensure the operating system is configured to enable DAC on hardlinks - Sections Modified: Remediation Procedure; Audit Procedure                           |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.5.16 - Ensure the operating system restricts exposed kernel pointer addresses access - Sections Modified: Description; Remediation Procedure; Audit Procedure     |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.5.17 - Ensure the operating system is configured to restrict access to the kernel message buffer - Sections Modified: Remediation Procedure; Audit Procedure      |

| Date       | Version | Changes for this version                                                                                                                                                                                         |
|------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.5.19 - Ensure the operating system is configured to prevent kernel profiling by unprivileged users - Sections Modified: Remediation Procedure; Audit Procedure                         |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.5.20 - Ensure the operating system restricts usage of ptrace to descendant processes - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure     |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.5.21 - Ensure the operating system prevents privilege escalation through the kernel by disabling access to the bpf syscall - Sections Modified: Remediation Procedure; Audit Procedure |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.5.22 - Ensure the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed - Sections Modified: Remediation Procedure                                   |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.6.9 - Ensure PKI-based authentication has valid certificates - Sections Modified: Description; Rationale Statement; Audit Procedure                                                    |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.6.10 - Ensure system-wide crypto policies are in effect - Sections Modified: Audit Procedure                                                                                           |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.6.11 - Ensure the operating system implements certificate status checking for multifactor authentication - Sections Modified: Remediation Procedure                                    |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.6.13 - Ensure the OpenSSL library is configured to use only DoD-approved TLS encryption - Sections Modified: Remediation Procedure; Audit Procedure                                    |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.7.1 - Ensure message of the day is configured properly - Sections Modified: Remediation Procedure                                                                                      |

| Date       | Version | Changes for this version                                                                                                                                                                                                                      |
|------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.7.2 - Ensure local login warning banner is configured properly - Sections Modified: Remediation Procedure                                                                                                           |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.7.3 - Ensure remote login warning banner is configured properly - Sections Modified: Remediation Procedure                                                                                                          |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.7.7 - Ensure the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a command line user logon - Sections Modified: Assessment Status |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.8.1 - Ensure GNOME Display Manager is removed - Sections Modified: Assessment Status; Impact Statement; Remediation Procedure; Audit Procedure                                                                      |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.8.2 - Ensure GDM login banner is configured - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure                                                                                        |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 1.8.14 - Ensure the operating system disables the user logon list for graphical user interfaces - Sections Modified: Remediation Procedure                                                                            |
| 11/25/2024 | 2.0.0   | UPDATED SECTION: 2 - Services - Sections Modified: Description                                                                                                                                                                                |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 2.2.4 - Ensure telnet client is not installed - Sections Modified: Remediation Procedure; Audit Procedure                                                                                                             |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 2.3.1 - Ensure time synchronization is in use - Sections Modified: Assessment Status; Description; Remediation Procedure; Audit Procedure                                                                             |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 2.3.2 - Ensure chrony is configured - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure                                                                                     |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 2.3.5 - Ensure the operating system disables network management of the chrony daemon - Sections Modified: Audit Procedure                                                                                             |

| Date       | Version | Changes for this version                                                                                                                                                       |
|------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | UPDATED SECTION: 2.4.1 - Configure cron - Sections Modified: Description                                                                                                       |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 2.4.1.2 - Ensure permissions on /etc/crontab are configured - Sections Modified: Remediation Procedure; Audit Procedure                                |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 2.4.1.3 - Ensure permissions on /etc/cron.hourly are configured - Sections Modified: Remediation Procedure; Audit Procedure                            |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 2.4.1.4 - Ensure permissions on /etc/cron.daily are configured - Sections Modified: Remediation Procedure; Audit Procedure                             |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 2.4.1.5 - Ensure permissions on /etc/cron.weekly are configured - Sections Modified: Description; Remediation Procedure; Audit Procedure               |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 2.4.1.6 - Ensure permissions on /etc/cron.monthly are configured - Sections Modified: Description; Remediation Procedure; Audit Procedure              |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 2.4.1.7 - Ensure permissions on /etc/cron.d are configured - Sections Modified: Description; Remediation Procedure; Audit Procedure                    |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 3.1.2 - Ensure wireless interfaces are disabled - Sections Modified: Profile; Description; Rationale Statement; Remediation Procedure; Audit Procedure |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 3.1.4 - Ensure network interfaces are not in promiscuous mode - Sections Modified: Assessment Status                                                   |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 3.3.2 - Ensure packet redirect sending is disabled - Sections Modified: Impact Statement; Remediation Procedure; Audit Procedure                       |

| Date       | Version | Changes for this version                                                                                                                                                                |
|------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 3.3.8 - Ensure source routed packets are not accepted - Sections Modified: Profile; Rationale Statement; Remediation Procedure; Audit Procedure                 |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 3.3.9 - Ensure suspicious packets are logged - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure                                   |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 4.1.3 - Ensure firewall service is enabled and running - Sections Modified: Profile                                                                             |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 4.1.7 - Ensure firewall is installed - Sections Modified: Remediation Procedure; Audit Procedure"                                                               |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 4.1.8 - Ensure firewall is configured to employ a deny-all                                                                                                      |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 4.1.1.1 - Ensure nftables base chains exist - Sections Modified: Description; Impact Statement; Remediation Procedure; Audit Procedure                          |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 4.1.1.3 - Ensure firewall drops unnecessary services and ports - Sections Modified: Description; Remediation Procedure; Audit Procedure                         |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 4.1.1.5 - Ensure nftables default deny firewall policy - Sections Modified: Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure       |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.1.2 - Ensure permissions on /etc/ssh/sshd_config are configured - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.1.3 - Ensure permissions on SSH private host key files are configured - Sections Modified: Remediation Procedure; Audit Procedure                             |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.1.4 - Ensure permissions on SSH public host key files are configured - Sections Modified: Remediation Procedure; Audit Procedure                              |

| Date       | Version | Changes for this version                                                                                                                                                                      |
|------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.1.28 - Ensure the SSH server is configured to use only MACs employing FIPS 140-2-approved algorithms - Sections Modified: Remediation Procedure; Audit Procedure    |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.1.29 - Ensure the SSH server is configured to use only ciphers employing FIPS 140-2-approved algorithms - Sections Modified: Remediation Procedure; Audit Procedure |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.1.31 - Ensure the SSH server uses strong entropy - Sections Modified: Audit Procedure                                                                               |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.1.39 - Ensure SSH is loaded and active - Sections Modified: Remediation Procedure; Audit Procedure                                                                  |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.2.1 - Ensure sudo is installed - Sections Modified: Description; Rationale Statement; Audit Procedure                                                               |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.2.3 - Ensure sudo commands use pty - Sections Modified: Description; Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure                  |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.2.4 - Ensure sudo log file exists - Sections Modified: Description; Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure                   |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.2.8 - Ensure the sudoers security policy is configured to use the invoking user's password for privilege escalation - Sections Modified: Remediation Procedure      |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.2.10 - Ensure access to the su command is restricted - Sections Modified: Description; Remediation Procedure; Audit Procedure                                       |
| 11/25/2024 | 2.0.0   | UPDATED SECTION: 5.3.2 - Configure authselect - Sections Modified: Description                                                                                                                |

| Date       | Version | Changes for this version                                                                                                                                                                                                    |
|------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.3.3.2.8 - Ensure the operating system enforces a minimum 15-character password length - Sections Modified: Audit Procedure                                                                        |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.3.3.6.1 - Ensure the operating system uses multifactor authentication for local access to accounts - Sections Modified: Audit Procedure                                                           |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.3.3.6.2 - Ensure SSSD prohibits the use of cached authentications after one day - Sections Modified: Audit Procedure                                                                              |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.4.1.6 - Ensure all users last password change date is in the past - Sections Modified: Rationale Statement; Audit Procedure                                                                       |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.4.2.1 - Ensure root is the only UID 0 account - Sections Modified: Profile; Rationale Statement; Remediation Procedure; Audit Procedure                                                           |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.4.3.4 - Ensure emergency accounts have been provisioned with an expiration date of 72 hours - Sections Modified: Remediation Procedure; Audit Procedure                                           |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.4.3.7 - Ensure the operating system enforces a 60-day maximum password lifetime for new user accounts - Sections Modified: Audit Procedure                                                        |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.4.3.8 - Ensure the umask default for installed shells is 077" - Sections Modified: Remediation Procedure; Audit Procedure"                                                                        |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.4.3.9 - Ensure the default umask for all local interactive users is 077" - Sections Modified: Audit Procedure"                                                                                    |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.4.3.12 - Ensure the operating system's shell initialization file is configured to start each shell with the tmux terminal multiplexer - Sections Modified: Remediation Procedure; Audit Procedure |



| Date       | Version | Changes for this version                                                                                                                                                                                          |
|------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 5.4.3.13 - Ensure the operating system enables the user to initiate a session lock - Sections Modified: Remediation Procedure; Audit Procedure                                            |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.1.1 - Ensure AIDE is installed - Sections Modified: Profile; Description; Remediation Procedure                                                                                         |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.1.2 - Ensure filesystem integrity is regularly checked - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure                                                 |
| 11/25/2024 | 2.0.0   | UPDATED SECTION: 6.2.1 - Configure journald - Sections Modified: Description                                                                                                                                      |
| 11/25/2024 | 2.0.0   | UPDATED SECTION: 6.2.2 - Configure rsyslog - Sections Modified: Description                                                                                                                                       |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.2.2.1 - Ensure rsyslog is installed - Sections Modified: Profile; Description; Remediation Procedure; Audit Procedure                                                                   |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.2.2.4 - Ensure journald is configured to send logs to rsyslog - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure                             |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.2.2.7 - Ensure rsyslog is configured to send logs to a remote log host - Sections Modified: Assessment Status; Description; Rationale Statement; Remediation Procedure; Audit Procedure |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.3.1.2 - Ensure auditing for processes that start prior to auditd is enabled - Sections Modified: Profile; Remediation Procedure; Audit Procedure                                        |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.3.1.3 - Ensure audit_backlog_limit is sufficient - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure                                          |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.3.2.1 - Ensure audit log storage size is configured - Sections Modified: Audit Procedure                                                                                                |

| Date       | Version | Changes for this version                                                                                                                                                                                      |
|------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.3.2.3 - Ensure system is disabled when audit logs are full - Sections Modified: Profile; Description; Impact Statement; Remediation Procedure; Audit Procedure                      |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.3.2.5 - Ensure the operating system allocates audit record storage capacity - Sections Modified: Audit Procedure                                                                    |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.3.3.1 - Ensure changes to system administration scope (sudoers) is collected - Sections Modified: Profile; Description; Rationale Statement; Remediation Procedure; Audit Procedure |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.3.3.4 - Ensure events that modify date and time information are collected - Sections Modified: Description; Remediation Procedure; Audit Procedure                                  |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.3.3.5 - Ensure events that modify the system's network environment are collected - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure      |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.3.3.8 - Ensure events that modify user/group information are collected - Sections Modified: Profile; Description; Remediation Procedure; Audit Procedure                            |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.3.3.9 - Ensure discretionary access control permission modification events are collected - Sections Modified: Profile; Description; Remediation Procedure; Audit Procedure          |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.3.3.10 - Ensure successful file system mounts are collected - Sections Modified: Profile; Rationale Statement; Remediation Procedure; Audit Procedure                               |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.3.3.11 - Ensure session initiation information is collected - Sections Modified: Description; Remediation Procedure; Audit Procedure                                                |

| Date       | Version | Changes for this version                                                                                                                                                                                        |
|------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.3.3.12 - Ensure login and logout events are collected - Sections Modified: Profile; Description; Remediation Procedure; Audit Procedure                                               |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.3.3.13 - Ensure file deletion events by users are collected - Sections Modified: Profile; Description; Remediation Procedure; Audit Procedure                                         |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.3.3.14 - Ensure events that modify the system's Mandatory Access Controls are collected - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.3.3.20 - Ensure the audit configuration is immutable - Sections Modified: Profile; Description; Remediation Procedure; Audit Procedure                                                |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 6.3.3.43 - Ensure the audit system prevents unauthorized changes to logon UIDs - Sections Modified: Remediation Procedure; Audit Procedure                                              |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 7.1.1 - Ensure permissions on /etc/passwd are configured - Sections Modified: Remediation Procedure; Audit Procedure                                                                    |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 7.1.2 - Ensure permissions on /etc/passwd- are configured - Sections Modified: Remediation Procedure; Audit Procedure                                                                   |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 7.1.3 - Ensure permissions on /etc/group are configured - Sections Modified: Remediation Procedure; Audit Procedure                                                                     |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 7.1.4 - Ensure permissions on /etc/group- are configured - Sections Modified: Remediation Procedure; Audit Procedure                                                                    |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 7.1.5 - Ensure permissions on /etc/shadow are configured - Sections Modified: Remediation Procedure; Audit Procedure                                                                    |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 7.1.6 - Ensure permissions on /etc/shadow- are configured - Sections Modified: Remediation Procedure; Audit Procedure                                                                   |

| Date       | Version | Changes for this version                                                                                                                       |
|------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------|
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 7.1.7 - Ensure permissions on /etc/gshadow are configured - Sections Modified: Remediation Procedure; Audit Procedure  |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 7.1.8 - Ensure permissions on /etc/gshadow- are configured - Sections Modified: Remediation Procedure; Audit Procedure |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 7.2.3 - Ensure all groups in /etc/passwd exist in /etc/group - Sections Modified: Audit Procedure                      |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 7.2.4 - Ensure shadow group is empty - Sections Modified: Audit Procedure                                              |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 7.2.5 - Ensure no duplicate UIDs exist - Sections Modified: Rationale Statement; Audit Procedure                       |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 7.2.6 - Ensure no duplicate GIDs exist - Sections Modified: Audit Procedure                                            |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 7.2.7 - Ensure no duplicate user names exist - Sections Modified: Audit Procedure                                      |
| 11/25/2024 | 2.0.0   | UPDATED RECOMMENDATION: 7.2.8 - Ensure no duplicate group names exist - Sections Modified: Audit Procedure                                     |