

CIS Amazon Linux 2 STIG Benchmark

v2.0.0 - 11-29-2021

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/>

Table of Contents

Terms of Use	1
Overview	19
Intended Audience	19
Consensus Guidance.....	19
Assessment Status.....	20
Profile Definitions	21
Acknowledgements	22
Recommendations	23
1 Initial Setup	23
1.1 Filesystem Configuration	24
1.1.1 Disable unused filesystems.....	25
1.1.1.1 Ensure mounting of cramfs filesystems is disabled (Automated)	26
1.1.1.2 Ensure mounting of squashfs filesystems is disabled (Automated).....	28
1.1.1.3 Ensure mounting of udf filesystems is disabled (Automated).....	30
1.1.2 Ensure /tmp is configured (Automated)	32
1.1.3 Ensure noexec option set on /tmp partition (Automated)	36
1.1.4 Ensure nodev option set on /tmp partition (Automated)	38
1.1.5 Ensure nosuid option set on /tmp partition (Automated)	40
1.1.6 Ensure /dev/shm is configured (Automated)	43
1.1.7 Ensure noexec option set on /dev/shm partition (Automated).....	45
1.1.8 Ensure nodev option set on /dev/shm partition (Automated)	47
1.1.9 Ensure nosuid option set on /dev/shm partition (Automated)	49
1.1.10 Ensure separate partition exists for /var (Automated)	51
1.1.11 Ensure separate partition exists for /var/tmp (Automated).....	53
1.1.12 Ensure /var/tmp partition includes the noexec option (Automated).....	55
1.1.13 Ensure /var/tmp partition includes the nodev option (Automated)	57
1.1.14 Ensure /var/tmp partition includes the nosuid option (Automated)	59
1.1.15 Ensure separate partition exists for /var/log (Automated).....	61
1.1.16 Ensure separate partition exists for /var/log/audit (Automated).....	63

1.1.17 Ensure separate partition exists for /home (Automated).....	65
1.1.18 Ensure /home partition includes the nodev option (Automated)	67
1.1.19 Ensure nosuid is set on users' home directories. (Automated)	69
1.1.20 Ensure removable media partitions include noexec option (Automated)..	71
1.1.21 Ensure nodev option set on removable media partitions (Automated)	73
1.1.22 Ensure nosuid option set on removable media partitions (Automated).....	75
1.1.23 Ensure noexec option is configured for NFS. (Automated)	77
1.1.24 Ensure nosuid option is set for NFS (Automated)	79
1.1.25 Ensure sticky bit is set on all world-writable directories (Automated)	81
1.1.26 Ensure all world-writable directories are group-owned. (Automated)	83
1.1.27 Disable Automounting (Automated)	85
1.1.28 Disable USB Storage (Automated)	88
1.2 Configure Software Updates	91
1.2.1 Ensure GPG keys are configured (Manual)	92
1.2.2 Ensure package manager repositories are configured (Manual)	94
1.2.3 Ensure gpgcheck is globally activated (Automated)	96
1.2.4 Ensure software packages have been digitally signed by a Certificate Authority (CA) (Automated).....	98
1.2.5 Ensure removal of software components after update (Automated)	101
1.2.6 Ensure the version of the operating system is an active vendor supported release (Manual).....	103
1.3 Filesystem Integrity Checking.....	105
1.3.1 Ensure AIDE is installed (Automated).....	106
1.3.2 Ensure filesystem integrity is regularly checked (Automated)	108
1.3.3 Ensure AIDE is configured to verify ACLs (Manual).....	111
1.3.4 Ensure AIDE is configured to verify XATTRS (Manual)	113
1.3.5 Ensure AIDE is configured to use FIPS 140-2 (Manual)	115
1.4 Secure Boot Settings	117
1.4.1 Ensure bootloader password is set (Automated).....	118
1.4.2 Ensure permissions on bootloader config are configured (Automated).....	122
1.4.3 Ensure authentication required for single user mode (Automated)	125

1.4.4 Ensure boot loader does not allow removable media (Automated).....	127
1.4.5 Ensure version 7.2 or newer booted with a BIOS have a unique name for the grub superusers account (Manual).....	130
1.4.6 Ensure version 7.2 or newer booted with UEFI have a unique name for the grub superusers account (Manual).....	132
1.5 Additional Process Hardening	134
1.5.1 Ensure core dumps are restricted (Automated).....	135
1.5.2 Ensure XD/NX support is enabled (Automated)	137
1.5.3 Ensure address space layout randomization (ASLR) is enabled (Automated)	139
1.5.4 Ensure prelink is not installed (Automated).....	141
1.5.5 Ensure number of concurrent sessions is limited (Automated).....	143
1.5.6 Ensure the Ctrl-Alt-Delete key sequence is disabled. (Automated)	145
1.5.7 Ensure kernel core dumps are disabled. (Automated)	148
1.5.8 Ensure DNS is servers are configured (Automated)	150
1.5.9 Ensure NIST FIPS-validated cryptography is configured (Automated).....	152
1.6 Mandatory Access Control.....	157
1.6.1 Configure SELinux	158
1.6.1.1 Ensure SELinux is installed (Automated)	159
1.6.1.2 Ensure SELinux is not disabled in bootloader configuration (Automated)	161
1.6.1.3 Ensure SELinux policy is configured (Automated)	163
1.6.1.4 Ensure the SELinux mode is enforcing or permissive (Automated)	165
1.6.1.5 Ensure the SELinux mode is enforcing (Automated)	168
1.6.1.6 Ensure no unconfined services exist (Automated)	171
1.6.1.7 Ensure SETroubleshoot is not installed (Automated)	173
1.6.1.8 Ensure the MCS Translation Service (mcstrans) is not installed (Automated).....	175
1.6.1.9 Ensure non-privileged users are prevented from executing privileged functions (Manual)	177
1.6.1.10 Ensure system device files are labeled. (Manual)	181
1.7 Command Line Warning Banners.....	184

1.7.1 Ensure message of the day is configured properly (Automated).....	185
1.7.2 Ensure local login warning banner is configured properly (Automated)....	187
1.7.3 Ensure the Standard Mandatory DoD Notice and Consent Banner are configured (Automated).....	189
1.7.4 Ensure remote login warning banner is configured properly (Automated)	192
1.7.5 Ensure permissions on /etc/motd are configured (Automated)	194
1.7.6 Ensure permissions on /etc/issue are configured (Automated)	196
1.7.7 Ensure permissions on /etc/issue.net are configured (Automated).....	197
1.7.8 Ensure the Standard Mandatory DoD Notice and Consent Banner are configured (Manual)	199
1.8 GNOME Display Manager	204
1.8.1 Ensure GDM login banner is configured (Manual).....	205
1.8.2 Ensure Standard Mandatory DoD Notice and Consent Banner displayed via a graphical user logon (Manual).....	208
1.8.3 Ensure GDM session lock is enabled (Automated)	212
1.8.4 Ensure the graphical user Ctrl-Alt-Delete key sequence is disabled (Automated).....	214
1.8.5 Ensure users must authenticate users using MFA via a graphical user logon (Automated).....	216
1.8.6 Ensure GNOME Screensaver period of inactivity is configured (Automated)	218
1.8.7 Ensure screensaver lock-enabled is set (Automated)	220
1.8.8 Ensure overriding the screensaver lock-delay setting is prevented (Automated).....	223
1.8.9 Ensure session idle-delay settings is enforced (Automated).....	226
1.8.10 Ensure GNOME Idle activation is set (Automated)	228
1.8.11 Ensure the screensaver idle-activation-enabled setting (Automated)	230
1.8.12 Ensure GNOME Lock Delay is configured (Automated)	233
1.8.13 Ensure automatic logon via GUI is not allowed (Automated).....	235
1.8.14 Ensure unrestricted logon is not allowed (Automated).....	237
1.8.15 Ensure graphical user interface automounter is disabled (Automated) ...	239

1.9 Ensure updates, patches, and additional security software are installed (Manual)	243
1.10 Ensure required packages for multifactor authentication are installed (Automated)	245
1.11 Ensure anti-virus is installed and running (Manual)	248
1.12 Ensure host-based intrusion detection tool is used (Manual)	250
2 Services.....	252
2.1 inetd Services.....	253
2.1.1 Ensure xinetd is not installed (Automated).....	254
2.2 Special Purpose Services	256
2.2.1 Time Synchronization	257
2.2.1.1 Ensure time synchronization is in use (Manual)	258
2.2.1.2 Ensure chrony is configured (Automated).....	260
2.2.1.3 Ensure ntp is configured (Automated)	262
2.2.1.4 Ensure internal information system clocks are synchronizing (Automated)	265
2.2.2 Ensure X11 Server components are not installed (Automated).....	269
2.2.3 Ensure Avahi Server is not installed (Automated)	271
2.2.4 Ensure CUPS is not installed (Automated).....	273
2.2.5 Ensure DHCP Server is not installed (Automated)	275
2.2.6 Ensure LDAP server is not installed (Automated)	277
2.2.7 Ensure DNS Server is not installed (Automated)	279
2.2.8 Ensure FTP Server is not installed (Automated)	281
2.2.9 Ensure HTTP server is not installed (Automated).....	283
2.2.10 Ensure IMAP and POP3 server is not installed (Automated).....	285
2.2.11 Ensure Samba is not installed (Automated)	287
2.2.12 Ensure HTTP Proxy Server is not installed (Automated)	289
2.2.13 Ensure net-snmp is not installed (Automated)	291
2.2.14 Ensure NIS server is not installed (Automated).....	293
2.2.15 Ensure telnet-server is not installed (Automated)	295

2.2.16 Ensure mail transfer agent is configured for local-only mode (Automated)	297
2.2.17 Ensure nfs-utils is not installed or the nfs-server service is masked (Automated)	299
2.2.18 Ensure rpcbind is not installed or the rpcbind services are masked (Automated)	301
2.2.19 Ensure rsync is not installed or the rsyncd service is masked (Automated)	304
2.2.20 Ensure the rsh package has been removed (Automated)	306
2.2.21 Ensure the TFTP server has not been installed (Automated)	308
2.2.22 Ensure TFTP daemon is configured to operate in secure mode (Automated)	310
2.2.23 Ensure default SNMP community strings don't exist (Automated)	312
2.2.24 Ensure NFS is configured to use RPCSEC_GSS (Automated)	314
2.2.25 Ensure unrestricted mail relaying is prevented (Automated)	316
2.2.26 Ensure ldap_tls_cacert is set for LDAP. (Automated)	318
2.2.27 Ensure ldap_id_use_start_tls is set for LDAP. (Automated)	320
2.2.28 Ensure ldap_tls_reqcert is set for LDAP (Automated)	322
2.3 Service Clients	324
2.3.1 Ensure NIS Client is not installed (Automated)	325
2.3.2 Ensure rsh client is not installed (Automated)	327
2.3.3 Ensure talk client is not installed (Automated)	329
2.3.4 Ensure telnet client is not installed (Automated)	331
2.3.5 Ensure LDAP client is not installed (Automated)	333
2.4 Ensure nonessential services are removed or masked (Manual)	335
3 Network Configuration	337
3.1 Disable unused network protocols and devices	338
3.1.1 Disable IPv6 (Manual)	339
3.1.2 Ensure wireless interfaces are disabled (Automated)	342
3.2 Network Parameters (Host Only)	345
3.2.1 Ensure IP forwarding is disabled (Automated)	346
3.2.2 Ensure packet redirect sending is disabled (Automated)	349

3.3 Network Parameters (Host and Router)	351
3.3.1 Ensure source routed packets are not accepted (Automated)	352
3.3.2 Ensure ICMP redirects are not accepted (Automated)	356
3.3.3 Ensure network interfaces are not in promiscuous mode (Manual)	360
3.3.4 Ensure secure ICMP redirects are not accepted (Automated)	362
3.3.5 Ensure suspicious packets are logged (Automated)	364
3.3.6 Ensure broadcast ICMP requests are ignored (Automated)	366
3.3.7 Ensure bogus ICMP responses are ignored (Automated)	368
3.3.8 Ensure Reverse Path Filtering is enabled (Automated)	370
3.3.9 Ensure TCP SYN Cookies is enabled (Automated)	373
3.3.10 Ensure IPv6 router advertisements are not accepted (Automated)	375
3.4 Uncommon Network Protocols	378
3.4.1 Ensure DCCP is disabled (Automated)	379
3.4.2 Ensure SCTP is disabled (Automated)	381
3.5 Firewall Configuration	383
3.5.1 Configure firewalld	384
3.5.1.1 Ensure firewalld is installed (Automated)	385
3.5.1.2 Ensure iptables-services not installed with firewalld (Automated)	387
3.5.1.3 Ensure nftables either not installed or masked with firewalld (Automated)	389
3.5.1.4 Ensure firewalld service enabled and running (Automated)	391
3.5.1.5 Ensure firewalld default zone is set (Automated)	393
3.5.1.6 Ensure network interfaces are assigned to appropriate zone (Manual) ..	396
3.5.1.7 Ensure firewalld drops unnecessary services and ports (Manual)	398
3.5.2 Configure nftables	400
3.5.2.1 Ensure nftables is installed (Automated)	403
3.5.2.2 Ensure firewalld is either not installed or masked with nftables (Automated)	405
3.5.2.3 Ensure iptables-services not installed with nftables (Automated)	407
3.5.2.4 Ensure iptables are flushed with nftables (Manual)	409
3.5.2.5 Ensure an nftables table exists (Automated)	411

3.5.2.6 Ensure nftables base chains exist (Automated)	413
3.5.2.7 Ensure nftables loopback traffic is configured (Automated)	415
3.5.2.8 Ensure nftables outbound and established connections are configured (Manual)	418
3.5.2.9 Ensure nftables default deny firewall policy (Automated)	420
3.5.2.10 Ensure nftables service is enabled (Automated)	422
3.5.2.11 Ensure nftables rules are permanent (Automated)	423
3.5.3 Configure iptables	426
3.5.3.1.1 Ensure iptables packages are installed (Automated)	428
3.5.3.1.2 Ensure nftables is not installed with iptables (Automated)	430
3.5.3.1.3 Ensure firewalld is either not installed or masked with iptables (Automated)	432
3.5.3.2.1 Ensure iptables loopback traffic is configured (Automated)	435
3.5.3.2.2 Ensure iptables outbound and established connections are configured (Manual)	437
3.5.3.2.3 Ensure iptables rules exist for all open ports (Automated)	439
3.5.3.2.4 Ensure iptables default deny firewall policy (Automated)	442
3.5.3.2.5 Ensure iptables rules are saved (Automated)	444
3.5.3.2.6 Ensure iptables is enabled and running (Automated)	447
3.5.3.3.1 Ensure ip6tables loopback traffic is configured (Automated)	450
3.5.3.3.2 Ensure ip6tables outbound and established connections are configured (Manual)	453
3.5.3.3.3 Ensure ip6tables firewall rules exist for all open ports (Automated)	456
3.5.3.3.4 Ensure ip6tables default deny firewall policy (Automated)	459
3.5.3.3.5 Ensure ip6tables rules are saved (Automated)	462
3.5.3.3.6 Ensure ip6tables is enabled and running (Automated)	466
3.5.4 Ensure IP tunnels are not configured (Automated)	468
4 Logging and Auditing	470
4.1 Configure System Accounting (auditd)	471
4.1.1 Ensure auditing is enabled	472
4.1.1.1 Ensure auditd is installed (Automated)	473

4.1.1.2 Ensure auditd service is enabled and running (Automated)	475
4.1.1.3 Ensure auditing for processes that start prior to auditd is enabled (Automated).....	477
4.1.2 Configure Data Retention	479
4.1.2.1 Ensure audit log storage size is configured (Automated)	480
4.1.2.2 Ensure audit logs are not automatically deleted (Automated)	482
4.1.2.3 Ensure audit system is set to single when the disk is full. (Automated) ..	484
4.1.2.4 Ensure system notification is sent out when volume is 75% full (Manual)	486
4.1.2.5 Ensure system is disabled when audit logs are full (Automated)	490
4.1.2.6 Ensure audit system action is defined for sending errors (Automated) ..	492
4.1.2.7 Ensure audit_backlog_limit is sufficient (Automated)	494
4.1.2.8 Ensure audit logs are stored on a different system. (Manual).....	496
4.1.2.9 Ensure audit logs on separate system are encrypted. (Automated)	498
4.1.2.10 Ensure the auditing processing failures are handled. (Automated)	500
4.1.2.11 Ensure off-load of audit logs. (Automated)	504
4.1.2.12 Ensure action is taken when audisp-remote buffer is full (Automated)	506
4.1.2.13 Ensure off-loaded audit logs are labeled. (Automated)	508
4.1.3 Configure auditd rules	510
4.1.3.1 Ensure events that modify date and time information are collected (Automated).....	511
4.1.3.2 Ensure system administrator command executions (sudo) are collected (Automated).....	514
4.1.3.3 Ensure session initiation information is collected (Automated)	517
4.1.3.4 Ensure events that modify the system's Mandatory Access Controls are collected (Automated)	520
4.1.3.5 Ensure events that modify the system's network environment are collected (Automated)	522
4.1.3.6 Ensure successful file system mounts are collected (Automated).....	525
4.1.3.7 Ensure kernel module loading and unloading is collected (Automated) .	528
4.1.3.8 Ensure changes to system administration scope (sudoers) is collected (Automated).....	532

4.1.3.9 Ensure file deletion events by users are collected (Automated)	535
4.1.3.10 Ensure use of privileged commands is collected (Automated)	539
4.1.3.11 Ensure unsuccessful unauthorized file access attempts are collected (Automated).....	542
4.1.3.12 Ensure discretionary access control permission modification events are collected (Automated)	546
4.1.3.13 Ensure login and logout events are collected (Automated)	551
4.1.3.14 Ensure events that modify user/group information are collected (Automated).....	554
4.1.3.15 Ensure all uses of the passwd command are audited. (Automated).....	557
4.1.3.16 Ensure auditing of the unix_chkpwd command (Automated)	560
4.1.3.17 Ensure audit of the gpasswd command (Automated).....	563
4.1.3.18 Ensure audit all uses of chage (Automated).....	566
4.1.3.19 Ensure audit all uses of the chsh command. (Automated)	569
4.1.3.20 Ensure audit the umount command (Automated).....	572
4.1.3.21 Ensure audit of postdrop command (Automated).....	575
4.1.3.22 Ensure audit of postqueue command. (Automated)	578
4.1.3.23 Ensure audit ssh-keysign command. (Automated)	581
4.1.3.24 Ensure audit of crontab command (Automated)	584
4.1.3.25 Ensure audit of kmod command (Automated).....	587
4.1.3.26 Ensure audit of the rmdir syscall (Automated)	589
4.1.3.27 Ensure audit of unlink syscall (Automated).....	592
4.1.3.28 Ensure audit unlinkat syscall (Automated).....	595
4.1.3.29 Ensure audit pam_timestamp_check command (Automated)	598
4.1.3.30 Ensure audit of the finit_module syscall (Automated).....	600
4.1.3.31 Ensure audit of the create_module syscall (Automated)	603
4.1.3.32 Ensure auditing of all privileged functions (Automated)	606
4.1.3.33 Ensure audit of semanage command (Automated).....	608
4.1.3.34 Ensure audit of the setsebool command. (Automated)	611
4.1.3.35 Ensure audit of the chcon command (Automated).....	614
4.1.3.36 Ensure audit of the userhelper command (Automated)	617

4.1.3.37 Ensure audit of the mount command and syscall (Automated)	620
4.1.3.38 Ensure audit of the su command (Automated)	623
4.1.3.39 Ensure audit of setfiles command (Automated)	626
4.1.3.40 Ensure audit all uses of the newgrp command (Automated)	629
4.1.3.41 Ensure the audit configuration is immutable (Automated)	632
4.1.4 Configure auditd file access	634
4.1.4.1 Ensure Audit logs are owned by root and mode 0600 or less permissive (Automated)	635
4.2 Configure Logging	638
4.2.1 Configure rsyslog	639
4.2.1.1 Ensure rsyslog is installed (Automated)	640
4.2.1.2 Ensure rsyslog Service is enabled and running (Automated)	642
4.2.1.3 Ensure rsyslog default file permissions configured (Automated)	644
4.2.1.4 Ensure logging is configured (Manual)	646
4.2.1.5 Ensure rsyslog is configured to send logs to a remote log host (Automated)	649
4.2.1.6 Ensure remote rsyslog messages are only accepted on designated log hosts. (Manual)	652
4.2.2 Configure journald	655
4.2.2.1 Ensure journald is configured to send logs to rsyslog (Automated)	656
4.2.2.2 Ensure journald is configured to compress large log files (Automated) ..	658
4.2.2.3 Ensure journald is configured to write logfiles to persistent disk (Automated)	660
4.2.3 Ensure logrotate is configured (Manual)	662
4.2.4 Ensure permissions on all logfiles are configured (Manual)	664
5 Access, Authentication and Authorization	666
5.1 Configure time-based job schedulers	667
5.1.1 Ensure cron daemon is enabled and running (Automated)	668
5.1.2 Ensure permissions on /etc/crontab are configured (Automated)	670
5.1.3 Ensure permissions on /etc/cron.hourly are configured (Automated)	672
5.1.4 Ensure permissions on /etc/cron.daily are configured (Automated)	674

5.1.5 Ensure permissions on /etc/cron.weekly are configured (Automated)	676
5.1.6 Ensure permissions on /etc/cron.monthly are configured (Automated) ...	678
5.1.7 Ensure permissions on /etc/cron.d are configured (Automated)	680
5.1.8 Ensure cron is restricted to authorized users (Automated)	682
5.1.9 Ensure at is restricted to authorized users (Automated).....	685
5.2 Configure sudo	687
5.2.1 Ensure sudo is installed (Automated)	688
5.2.2 Ensure sudo commands use pty (Automated)	690
5.2.3 Ensure sudo log file exists (Automated)	692
5.2.4 Ensure users must provide password for escalation (Automated).....	694
5.2.5 Ensure users must re-authenticate for privilege escalation (Automated) ..	697
5.2.6 Ensure the sudoers file restricts sudo access to authorized personnel (Automated).....	700
5.2.7 Ensure sudo authentication timeout is configured (Automated)	702
5.2.8 Ensure users password required for privilege escalation when using sudo (Automated).....	704
5.3 Configure SSH Server	706
5.3.1 Ensure SSH is installed (Automated)	707
5.3.2 Ensure SSH is running (Automated).....	709
5.3.3 Ensure permissions on /etc/ssh/sshd_config are configured (Automated)	711
5.3.4 Ensure permissions on SSH private host key files are configured (Automated).....	713
5.3.5 Ensure permissions on SSH public host key files are configured (Automated)	716
5.3.6 Ensure SSH access is limited (Automated)	719
5.3.7 Ensure SSH LogLevel is appropriate (Automated)	722
5.3.8 Ensure SSH X11 forwarding is disabled (Automated).....	724
5.3.9 Ensure SSH MaxAuthTries is set to 4 or less (Automated)	726
5.3.10 Ensure SSH IgnoreRhosts is enabled (Automated)	728
5.3.11 Ensure SSH HostbasedAuthentication is disabled (Automated)	730
5.3.12 Ensure SSH root login is disabled (Automated)	732

5.3.13 Ensure SSH PermitEmptyPasswords is disabled (Automated).....	734
5.3.14 Ensure SSH PermitUserEnvironment is disabled (Automated)	736
5.3.15 Ensure only strong Ciphers are used (Automated).....	738
5.3.16 Ensure only FIPS 140-2 ciphers are used for SSH (Automated)	742
5.3.17 Ensure only strong MAC algorithms are used (Automated).....	745
5.3.18 Ensure only strong Key Exchange algorithms are used (Automated)	749
5.3.19 Ensure SSH Idle Timeout Interval is configured (Automated)	752
5.3.20 Ensure SSH LoginGraceTime is set to one minute or less (Automated)	755
5.3.21 Ensure SSH warning banner is configured (Automated).....	757
5.3.22 Ensure SSH PAM is enabled (Automated)	759
5.3.23 Ensure SSH AllowTcpForwarding is disabled (Automated).....	761
5.3.24 Ensure SSH MaxStartups is configured (Automated)	764
5.3.25 Ensure SSH MaxSessions is limited (Automated).....	766
5.3.26 Ensure RSA rhosts authentication is not allowed (Automated)	768
5.3.27 Ensure Printlastlog is enabled (Automated)	770
5.3.28 Ensure SSH IgnoreUserKnownHosts is enabled (Automated)	772
5.3.29 Ensure SSH Protocol is set to 2 (Automated)	774
5.3.30 Ensure SSH does not permit GSSAPI (Automated)	776
5.3.31 Ensure SSH does not permit Kerberos authentication (Automated)	779
5.3.32 Ensure SSH performs checks of home directory configuration files (Automated).....	782
5.3.33 Ensure SSH uses privilege separation (Automated).....	784
5.3.34 Ensure SSH compressions setting is delayed (Automated)	786
5.3.35 Ensure SSH X11UseLocalhost is enabled (Automated)	788
5.3.36 Ensure no ".shosts" files exist on the system (Manual)	790
5.3.37 Ensure no "shosts.equiv" files exist on the system (Manual).....	792
5.4 Configure PAM.....	794
5.4.1 Ensure password creation requirements are configured (Automated)	795
5.4.2 Ensure lockout for failed password attempts is configured (Automated) ..	799
5.4.3 Ensure password hashing algorithm is SHA-512 (Automated).....	804
5.4.4 Ensure password reuse is limited (Automated)	806

5.4.5 Ensure system-auth is used when changing passwords (Automated)	808
5.4.6 Ensure no accounts are configured with blank or null passwords (Automated).....	810
5.4.7 Ensure minimum and maximum requirements are set for password changes (Automated).....	812
5.4.8 Ensure date and time of last successful logon (Automated)	816
5.4.9 Ensure multifactor authentication for access to privileged accounts (Automated).....	818
5.4.10 Ensure certificate status checking for PKI authentication (Automated)...	821
5.4.11 Ensure password prohibited reuse is at a minimum 5 (Automated)	824
5.4.12 Ensure accounts lock for a minimum of 15 minutes after three unsuccessful logon attempts within a 15-minute timeframe (Automated).....	826
5.4.13 Ensure lockout for unsuccessful root logon attempts (Automated)	830
5.5 User Accounts and Environment	833
5.5.1 Set Shadow Password Suite Parameters	834
5.5.1.1 Ensure password expiration is 365 days or less (Automated).....	835
5.5.1.2 Ensure minimum days between password changes is configured (Automated).....	837
5.5.1.3 Ensure password expiration warning days is 7 or more (Automated).....	839
5.5.1.4 Ensure inactive password lock is 30 days or less (Automated).....	841
5.5.1.5 Ensure all users last password change date is in the past (Automated) ..	843
5.5.1.6 Ensure shadow file is configured to use only encrypted representations of passwords (Automated).....	844
5.5.1.7 Ensure password expiration is 60 Day maximum for new users (Automated).....	846
5.5.1.8 Ensure password expiration is 60 Day maximum for existing passwords (Automated).....	848
5.5.1.9 Ensure inactive password lock is 0 days (Automated).....	850
5.5.1.10 Ensure delay between logon prompts on failure (Automated)	852
5.5.2 Ensure system accounts are secured (Automated)	854
5.5.3 Ensure default group for the root account is GID 0 (Automated).....	856
5.5.4 Ensure default user shell timeout is configured (Automated)	858

5.5.5 Ensure default user umask is configured (Automated)	861
5.5.6 Ensure user and group account administration utilities are configured to store only encrypted representations of passwords (Automated)	866
5.5.7 Ensure multi-factor authentication is enable for users (Automated)	868
5.5.8 Ensure Default user umask is 077 (Automated).....	871
5.5.9 Ensure local interactive user accounts umask is 077 (Automated)	873
5.5.10 Ensure upon user creation a home directory is assigned. (Automated) ...	876
5.6 Ensure root login is restricted to system console (Manual)	878
5.7 Ensure access to the su command is restricted (Automated)	880
6 System Maintenance.....	882
6.1 System File Permissions.....	883
6.1.1 Audit system file permissions (Manual)	884
6.1.2 Ensure permissions on /etc/passwd are configured (Automated)	887
6.1.3 Ensure permissions on /etc/passwd- are configured (Automated).....	889
6.1.4 Ensure permissions on /etc/shadow are configured (Automated)	891
6.1.5 Ensure permissions on /etc/shadow- are configured (Automated)	893
6.1.6 Ensure permissions on /etc/gshadow- are configured (Automated)	895
6.1.7 Ensure permissions on /etc/gshadow are configured (Automated).....	897
6.1.8 Ensure permissions on /etc/group are configured (Automated).....	899
6.1.9 Ensure permissions on /etc/group- are configured (Automated)	901
6.1.10 Ensure no world writable files exist (Automated)	903
6.1.11 Ensure no unowned files or directories exist (Automated)	905
6.1.12 Ensure no ungrouped files or directories exist (Automated)	907
6.1.13 Audit SUID executables (Manual)	909
6.1.14 Audit SGID executables (Manual)	911
6.1.15 Ensure the file permissions ownership and group membership of system files and commands match the vendor values (Manual).....	913
6.1.16 Ensure all world-writable directorys are owned by root, sys, bin, or an application User Identifier (Manual).....	915
6.2 User and Group Settings	917
6.2.1 Ensure accounts in /etc/passwd use shadowed passwords (Automated) .	918

6.2.2 Ensure /etc/shadow password fields are not empty (Automated)	920
6.2.3 Ensure all groups in /etc/passwd exist in /etc/group (Automated)	922
6.2.4 Ensure shadow group is empty (Automated)	924
6.2.5 Ensure no duplicate user names exist (Automated)	926
6.2.6 Ensure no duplicate group names exist (Automated)	928
6.2.7 Ensure no duplicate UIDs exist (Automated)	930
6.2.8 Ensure no duplicate GIDs exist (Automated)	932
6.2.9 Ensure root is the only UID 0 account (Automated)	934
6.2.10 Ensure root PATH Integrity (Automated)	936
6.2.11 Ensure all users' home directories exist (Automated)	938
6.2.12 Ensure users own their home directories (Automated)	941
6.2.13 Ensure users' home directories permissions are 750 or more restrictive (Automated)	944
6.2.14 Ensure users' dot files are not group or world writable (Automated)	947
6.2.15 Ensure no users have .forward files (Automated)	949
6.2.16 Ensure no users have .netrc files (Automated)	951
6.2.17 Ensure no users have .rhosts files (Automated)	954
6.2.18 Ensure there are no unnecessary accounts (Manual)	956
6.2.19 Ensure all local interactive user home directories are group-owned (Automated)	958
6.2.20 Ensure that all files and directories contained in local interactive user home directories are owned by the user (Automated)	960
6.2.21 Ensure local interactive user is a member of the group owner. (Automated)	962
6.2.22 Ensure users' files and directories within the home directory permissions are 750 or more restrictive (Automated)	964
6.2.23 Ensure local interactive users' dot files for are owned by the user or root. (Automated)	966
6.2.24 Ensure local interactive users' dot files are group-owned by the users group or root. (Automated)	968
6.2.25 Ensure users' dot files have 0740 or less set. (Automated)	971

6.2.26 Ensure local interactive users' dot files executable paths resolve to the users home directory. (Manual).....	973
Appendix: Recommendation Summary Table	976
Appendix: Change History	991

Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Amazon Linux 2 systems running on AWS. This document was tested against Amazon Linux 2.

The guidance within broadly assumes that operations are being performed as the root user. Operations performed using sudo instead of the root user 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.

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.

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 Amazon Linux 2.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. 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.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<i><italic font in brackets></i>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

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 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 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 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

Rael Daruszka , Center for Internet Security
Bill Erickson
Dave Billing
Dominic Pace
Ely Pinto
Fredrik Silverskär
Joy Latten
Koen Laevens
Mark Birch
Martynas Brijunas
Robert Thomas
Tom Pietschmann
Vineetha Hari Pai
Anurag Pal
Bradley Hieber
Thomas Sjögren <https://github.com/konstruktoid>
James Trigg , U.S. Patent and Trademark Office
Kenneth Karlsson

Editor

Jonathan Lewis Christopherson
Eric Pinnell

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 Configuration

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, make sure the data has been copied over to the new partition, unmount it and then remove the data from the directory that was in the old partition. Otherwise it will still consume space in the old partition that will be masked when the new filesystem is mounted. For example, if a system is in single-user mode with no filesystems mounted and the administrator adds a lot of data to the `/tmp` directory, this data will still consume space in `/` once the `/tmp` filesystem is mounted unless it is removed first.

1.1.1 Disable unused filesystems

A number of 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.

1.1.1.1 Ensure mounting of cramfs filesystems is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 server. If this filesystem type is not needed, disable it.

Audit:

Run the following commands and verify the output is as indicated:

```
# modprobe -n -v cramfs | grep -E '(cramfs|install)'  
  
install /bin/true  
# lsmod | grep cramfs  
  
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

Example: `vim /etc/modprobe.d/cramfs.conf`

and add the following line:

```
install cramfs /bin/true
```

Run the following command to unload the `cramfs` module:

```
# rmmod cramfs
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.1.1.2 Ensure mounting of squashfs filesystems is disabled (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 (similar to `cramfs`). 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:

Disabling `squashfs` will prevent the use of `snap`. `Snap` is a package manager for Linux for installing `Snap` packages.

"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. When snaps are deployed on versions of Linux, the Ubuntu app store is used as default back-end, but other stores can be enabled as well.

Audit:

Run the following commands and verify the output is as indicated:

```
# modprobe -n -v squashfs | grep -E '(squashfs|install)'  
  
install /bin/true  
# lsmod | grep squashfs  
  
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

Example: `vi /etc/modprobe.d/squashfs.conf`

and add the following line:

```
install squashfs /bin/true
```

Run the following command to unload the `squashfs` module:

```
# rmmod squashfs
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.1.1.3 Ensure mounting of udf filesystems is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - 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.

Audit:

Run the following commands and verify the output is as indicated:

```
# modprobe -n -v udf | grep -E '(udf|install)'  
  
install /bin/true  
# lsmod | grep udf  
  
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

Example: `vi /etc/modprobe.d/udf.conf`

and add the following line:

```
install udf /bin/true
```

Run the following command to unload the `udf` module:

```
# rmmod udf
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.1.2 Ensure /tmp is configured (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.

Rationale:

Making `/tmp` its own file system allows an administrator to set 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 hardlink to a system `setuid` program and wait for it to be updated. Once the program was updated, the hardlink 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:

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

Running out of `/tmp` space is a problem regardless of what kind of filesystem lies under it, but in a default installation a disk-based `/tmp` will essentially have the whole disk available, as it 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.

Audit:

Run the following command and verify output shows `/tmp` to `tmpfs` or a system partition:

```
# findmnt -n /tmp  
  
/tmp    tmpfs    tmpfs    rw,nosuid,nodev,noexec
```

If `/etc/fstab` is used: run the following command and verify that `tmpfs` has been mounted to `tmpfs`, or a system partition has been created for `/tmp`

```
# grep -E '\s/tmp\s' /etc/fstab | grep -E -v '^\s*#'
tmpfs    /tmp      tmpfs     defaults,noexec,nosuid,nodev 0    0
```

OR If `systemd tmp.mount` file is used: run the following command and verify that `tmp.mount` is enabled:

```
# systemctl show "tmp.mount" | grep -i unitfilestate
UnitFileState=enabled
```

Remediation:

Create or update an entry for `/tmp` in either `/etc/fstab` **OR** in a `systemd tmp.mount` file:

If `/etc/fstab` is used: configure `/etc/fstab` as appropriate.

_ Example:_

```
tmpfs    /tmp    tmpfs    defaults,rw,nosuid,nodev,noexec,relatime    0 0
```

Run the following command to remount `/tmp`

```
# mount -o remount,noexec,nodev,nosuid /tmp
```

OR if `systemd tmp.mount` file is used: run the following command to create the file

`/etc/systemd/system/tmp.mount` if it doesn't exist:

```
# [ ! -f /etc/systemd/system/tmp.mount ] && cp -v  
/usr/lib/systemd/system/tmp.mount /etc/systemd/system/
```

Edit the file `/etc/systemd/system/tmp.mount`:

```
[Mount]  
What=tmpfs  
Where=/tmp  
Type=tmpfs  
Options=mode=1777,strictatime,noexec,nodev,nosuid
```

Run the following command to reload the `systemd` daemon:

```
# systemctl daemon-reload
```

Run the following command to unmask and start `tmp.mount`:

```
# systemctl --now unmask tmp.mount
```

References:

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>
2. <https://www.freedesktop.org/wiki/Software/systemd/APIFileSystems/>
3. CCI: CCI-000366: The organization implements the security configuration settings.
4. NIST SP 800-53 :: CM-6 b
5. NIST SP 800-53A :: CM-6.1 (iv)
6. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

- If an entry for /tmp exists in /etc/fstab it will take precedence over entries in the tmp.mount file._
- tmpfs can be resized using the size={size} parameter in /etc/fstab or on the Options line in the tmp.mount file. If we don't specify the size, it will be half the RAM._

Resize tmpfs examples:

/etc/fstab example:

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

tmp.mount example:

```
[Mount]
What=tmpfs
Where=/tmp
Type=tmpfs
Options=mode=1777,strictatime,size=2G,noexec,nodev,nosuid
```

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204496
Rule ID: SV-204496r603261_rule
STIG ID: RHEL-07-021340
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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 Ensure noexec option set on /tmp partition (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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`.

Audit:

Run the following command to verify the `noexec` option is set:

```
# findmnt -n /tmp | grep -Ev '\bnodev\b'
```

Nothing should be returned

Remediation:

Edit the `/etc/fstab` file **OR** the `/etc/systemd/system/local-fs.target.wants/tmp.mount` file:

IF `/etc/fstab` is used to mount `/tmp`

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/tmp` partition. See the `fstab(5)` manual page for more information.

Run the following command to remount `/tmp`:

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

OR if systemd is used to mount `/tmp`:

Edit `/etc/systemd/system/local-fs.target.wants/tmp.mount` to add `noexec` to the `/tmp` mount options:

```
[Mount]
Options=mode=1777,strictatime,noexec,nodev,nosuid
```

Run the following command to restart the systemd daemon:

```
# systemctl daemon-reload
```

Run the following command to restart `tmp.mount`

```
# systemctl restart tmp.mount
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process 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	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			

1.1.4 Ensure nodev option set on /tmp 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 `/tmp` filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices in `/tmp`.

Audit:

Run the following command and verify the `nodev` option is set:

```
# findmnt -n /tmp -n | grep -Ev '\bnodev\b'
```

Nothing should be returned

Remediation:

Edit the `/etc/fstab` file **OR** the `/etc/systemd/system/local-fs.target.wants/tmp.mount` file:

IF `/etc/fstab` is used to mount `/tmp`

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

Run the following command to remount `/tmp`:

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

OR if `systemd` is used to mount `/tmp`:

Edit `/etc/systemd/system/local-fs.target.wants/tmp.mount` to add `nodev` to the `/tmp` mount options:

```
[Mount]
Options=mode=1777,strictatime,noexec,nodev,nosuid
```

Run the following command to restart the `systemd` daemon:

```
# systemctl daemon-reload
```

Run the following command to restart `tmp.mount`

```
# systemctl restart tmp.mount
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.1.5 Ensure nosuid option set on /tmp 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 `/tmp` filesystem is only intended for temporary file storage, set this option to ensure that users cannot create `setuid` files in `/tmp`.

Audit:

Run the following command and verify the `nodev` option is set:

```
# findmnt -n /tmp -n | grep -Ev '\bnosuid\b'
```

Nothing should be returned

Remediation:

IF /etc/fstab is used to mount /tmp

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

Run the following command to remount `/tmp`:

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

OR if systemd is used to mount /tmp:

Edit `/etc/systemd/system/local-fs.target.wants/tmp.mount` to add `nosuid` to the `/tmp` mount options:

```
[Mount]
Options=mode=1777,strictatime,noexec,nodev,nosuid
```

Run the following command to restart the `systemd` daemon:

```
# systemctl daemon-reload
```

Run the following command to restart `tmp.mount`:

```
# systemctl restart tmp.mount
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	<u>13 Data Protection</u> Data Protection			

1.1.6 Ensure /dev/shm is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`/dev/shm` is a traditional shared memory concept. One program will create a memory portion, which other processes (if permitted) can access. Mounting `tmpfs` at `/dev/shm` is handled automatically by `systemd`.

Rationale:

Any user can upload and execute files inside the `/dev/shm` similar to the `/tmp` partition. Configuring `/dev/shm` allows an administrator to set 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 hardlink to a system `setuid` program and wait for it to be updated. Once the program was updated, the hardlink 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.

Audit:

Run the following command and verify output shows `/dev/shm` is mounted:

```
# findmnt -n /dev/shm
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,noexec,relatime,seclabel)
```

Run the following command and verify an entry for `/dev/shm` exists in `/etc/fstab`:

```
# grep -E '\s/dev/shm\s' /etc/fstab
tmpfs      /dev/shm   tmpfs      defaults,noexec,nodev,nosuid 0 0
```

Remediation:

Edit `/etc/fstab` and add or edit the following line:

```
tmpfs /dev/shm tmpfs defaults,noexec,nodev,nosuid,seclabel 0 0
```

Run the following command to remount `/dev/shm`:

```
# mount -o remount,noexec,nodev,nosuid /dev/shm
```

Additional Information:

- An entry for `/dev/shm` in `/etc/fstab` will take precedence.
- `tmpfs` can be resized using the `size={size}` parameter in `/etc/fstab`. If we don't specify the size, it will be half the RAM.

Resize `tmpfs` example:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	13 <u>Data Protection</u> Data Protection			

1.1.7 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:

Run the following command to verify that the `noexec` option is set:

```
# findmnt -n /dev/shm | grep -Ev '\bnoexec\b'
```

Nothing should be returned

Remediation:

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

Run the following command to remount `/dev/shm`:

```
# mount -o remount,noexec,nodev,nosuid /dev/shm
```

References:

1. CCI: CCI-001764: The information system prevents program execution in accordance with organization-defined policies regarding software program usage and restrictions, and/or rules authorizing the terms and conditions of software program usage.
2. NIST SP 800-53 Revision 4 :: CM-7 (2)

Additional Information:

`/dev/shm` is mounted automatically by `systemd`. `/dev/shm` needs to be added to `/etc/fstab` to add mount options even though it is already being mounted on boot.

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204486
Rule ID: SV-204486r603261_rule
STIG ID: RHEL-07-021024
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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.			

1.1.8 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:

Run the following command to verify that the `nodev` option is set:

```
# findmnt -n /dev/shm | grep -Ev '\bnodev\b'
```

Nothing should be returned

Remediation:

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.

Run the following command to remount `/dev/shm`:

```
# mount -o remount,noexec,nodev,nosuid /dev/shm
```

References:

1. CCI: CCI-001764: The information system prevents program execution in accordance with organization-defined policies regarding software program usage and restrictions, and/or rules authorizing the terms and conditions of software program usage.
2. NIST SP 800-53 Revision 4 :: CM-7 (2)

Additional Information:

`/dev/shm` is mounted automatically by `systemd`. `/dev/shm` needs to be added to `/etc/fstab` to add mount options even though it is already being mounted on boot.

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204486
Rule ID: SV-204486r603261_rule
STIG ID: RHEL-07-021024
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

1.1.9 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:

Run the following command to verify that the `nosuid` option is set:

```
# findmnt -n /dev/shm | grep -Ev '\bnosuid\b'
```

Nothing should be returned

Remediation:

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.

Run the following command to remount `/dev/shm`:

```
# mount -o remount,noexec,nodev,nosuid /dev/shm
```

References:

1. CCI: CCI-001764: The information system prevents program execution in accordance with organization-defined policies regarding software program usage and restrictions, and/or rules authorizing the terms and conditions of software program usage.
2. NIST SP 800-53 Revision 4 :: CM-7 (2)

Additional Information:

`/dev/shm` is mounted automatically by `systemd`. `/dev/shm` needs to be added to `/etc/fstab` to add mount options even though it is already being mounted on boot.

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204486
Rule ID: SV-204486r603261_rule
STIG ID: RHEL-07-021024
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

1.1.10 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:

Since the `/var` directory may contain world-writable files and directories, there is a risk of resource exhaustion if it is not bound to a separate partition.

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:

```
# findmnt /var

TARGET SOURCE      FSTYPE OPTIONS
/var   <device>   <fstype> rw,relatime,attr2,inode64,noquota
```

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. CCI: CCI-000366: The organization implements the security configuration settings.
3. NIST SP 800-53 :: CM-6 b
4. NIST SP 800-53A :: CM-6.1 (iv)
5. NIST SP 800-53 Revision 4 :: CM-6 b

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 multiuser mode.

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204494
Rule ID: SV-204494r603261_rule
STIG ID: RHEL-07-021320
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

1.1.11 Ensure separate partition exists for /var/tmp (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The `/var/tmp` directory is a world-writable directory used for temporary storage by all users and some applications and is intended for temporary files that are preserved across reboots.

Rationale:

Since the `/var/tmp` directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition. In addition, making `/var/tmp` its own file system allows an administrator to set the `noexec` option on the mount, making `/var/tmp` useless for an attacker to install executable code. It would also prevent an attacker from establishing a hardlink to a system `setuid` program and wait for it to be updated. Once the program was updated, the hardlink 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.

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:

```
# findmnt /var/tmp

TARGET    SOURCE    FSTYPE    OPTIONS
/var/tmp  <device>  <fstype>  rw,relatime,attr2,inode64,noquota
```

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.

Additional Information:

- `tmpfs` should not be used for `/var/tmp/`
- `tmpfs` is a temporary filesystem that resides in memory and/or swap partition(s)
- Files in `tmpfs` are automatically cleared at each bootup

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	13 <u>Data Protection</u> Data Protection			

1.1.12 Ensure /var/tmp partition includes the noexec option (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 `/var/tmp` partition exists, run the following command to verify that the `noexec` option is set:

```
# findmnt -n /var/tmp | grep -Ev '\bnoexec\b'
```

Nothing should be returned

Remediation:

For existing `/var/tmp` partitions, edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) of the `/var/tmp` entry. See the `fstab(5)` manual page for more information.

Run the following command to remount `/var/tmp`:

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


CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>2.6 Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			

1.1.13 Ensure /var/tmp partition includes the nodev option (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/tmp` filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices in `/var/tmp`.

Audit:

If a `/var/tmp` partition exists, run the following command to verify that the `nodev` option is set:

```
# findmnt -n /var/tmp | grep -Ev '\bnodev\b'
```

Nothing should be returned

Remediation:

For existing `/var/tmp` partitions, edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) of the `/var/tmp` entry. See the `fstab(5)` manual page for more information.

Run the following command to remount `/var/tmp`:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	<u>13 Data Protection</u> Data Protection			

1.1.14 Ensure /var/tmp partition includes the nosuid option (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/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 `/var/tmp` partition exists, run the following command to verify that the `nosuid` option is set:

```
# findmnt -n /var/tmp | grep -Ev '\bnosuid\b'
```

Nothing should be returned

Remediation:

For existing `/var/tmp` partitions, edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) of the `/var/tmp` entry. See the `fstab(5)` manual page for more information.

Run the following command to remount `/var/tmp`:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	<u>13 Data Protection</u> Data Protection			

1.1.15 Ensure separate partition exists for /var/log (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

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

Rationale:

There are two important reasons to ensure that system logs are stored on a separate partition: protection against resource exhaustion (since logs can grow quite large) and protection of audit data.

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 /var/log

TARGET    SOURCE    FSTYPE    OPTIONS
/var/log  <device>  <fstype>  rw,relatime,attr2,inode64,noquota
```

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/>

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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.			
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> 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> Ensure that all systems that store logs have adequate storage space for the logs generated.			

1.1.16 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:

There are two important reasons to ensure that data gathered by `auditd` is stored on a separate partition: protection against resource exhaustion (since the `audit.log` file can grow quite large) and protection of audit data. The audit daemon calculates how much free space is left and performs actions based on the results. If other processes (such as `syslog`) consume space in the same partition as `auditd`, it may not perform as desired.

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 /var/log/audit

TARGET          SOURCE      FSTYPE     OPTIONS
/var/log/audit <device> <fstype>   rw,relatime,attr2,inode64,noquota
```

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. CCI: CCI-000366: The organization implements the security configuration settings.
3. NIST SP 800-53 :: CM-6 b
4. NIST SP 800-53A :: CM-6.1 (iv)
5. NIST SP 800-53 Revision 4 :: CM-6 b

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 multiuser mode.

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204495
Rule ID: SV-204495r603261_rule
STIG ID: RHEL-07-021330
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> 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> Ensure that all systems that store logs have adequate storage space for the logs generated.			

1.1.17 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:

If the system is intended to support local users, create a separate partition for the `/home` directory to protect against resource exhaustion and restrict the type of files that can be stored under `/home`.

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 /home
TARGET SOURCE FSTYPE OPTIONS
/home <device> <fstype> rw,relatime,attr2,inode64,noquota
```

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/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	<u>13 Data Protection</u> Data Protection			

1.1.18 Ensure /home partition includes the nodev option (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 user partitions are not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices.

Audit:

If a `/home` partition exists, run the following command to verify that the `nodev` option is set:

```
# findmnt /home | grep -Ev '\bnodev\b'
```

Nothing should be returned

Remediation:

For existing `/home` partitions, edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) of the `/home` entry. See the `fstab(5)` manual page for more information.

Run the following command to remount `/home`:

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

Additional Information:

The actions in this recommendation refer to the `/home` partition, which is the default user partition. If you have created other user partitions, it is recommended that the Remediation and Audit steps be applied to these partitions as well.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	<u>13 Data Protection</u> Data Protection			

1.1.19 Ensure nosuid is set on users' home directories. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that file systems containing user home directories are mounted to prevent files with the `setuid` and `setgid` bit set from being executed.

Rationale:

The `nosuid` mount option causes the system to not 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. Find the file system(s) that contain the user home directories with the following command:
Note: If a separate file system has not been created for the user home directories (`user` home directories are mounted under `"/"`), this is not a finding as the `nosuid` option cannot be used on the `/` system.

```
# cut -d: -f 1,3,6 /etc/passwd | egrep ":[1-4][0-9]{3}"  
  
smithj:1001:/home/smithj  
thomasr:1002:/home/thomasr
```

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 0 2
```

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, refer to the remediation procedure below.

Remediation:

Configure the `/etc/fstab` to use the `nosuid` option on file systems that contain user home directories.

Example: `vim /etc/fstab`

Update any of the file systems listed without the `nosuid` option"

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

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204480
Rule ID: SV-204480r603838_rule
STIG ID: RHEL-07-021000
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

1.1.20 Ensure removable media partitions include noexec option (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 script and verify that the `noexec` option is set on all removable media partitions.

```
#!/usr/bin/bash

for rmpo in $(lsblk -o RM,MOUNTPOINT | awk -F " " '/1/ {print $2}'); do
    findmnt -n "$rmpo" | grep -Ev "\bnoexec\b"
done
```

Nothing should be returned

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	2.6 <u>Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			
v7	13 <u>Data Protection</u> Data Protection			

1.1.21 Ensure nodev option set on removable media partitions (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 script and verify that the `nodev` option is set on all removable media partitions.

```
#!/usr/bin/bash

for rmpo in $(lsblk -o RM,MOUNTPOINT | awk -F " " '1/ {print $2}'); do
    findmnt -n "$rmpo" | grep -Ev "\bnodev\b"
done
```

Nothing should be returned

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	<u>13 Data Protection</u> Data Protection			

1.1.22 Ensure nosuid option set on removable media partitions (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:

Run the following command and verify that the `nosuid` option is set on all removable media partitions.

```
#!/usr/bin/bash

for rmpo in $(lsblk -o RM,MOUNTPOINT | awk -F " " '{print $2}'); do
    findmnt -n "$rmpo" | grep -Ev "\bnosuid\b"
done
```

Nothing should be returned

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. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204481
Rule ID: SV-204481r603261_rule
STIG ID: RHEL-07-021010
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>14.6 Protect Information through Access Control Lists</u> 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.			

1.1.23 Ensure noexec option is configured for NFS. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent binary files from being executed on file systems that are being imported via Network File System (NFS).

Rationale:

The "noexec" mount option causes the system to not 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 are being NFS imported are configured with the `noexec` option. Find the file system(s) that contain the directories being imported with the following command:

```
# more /etc/fstab | grep nfs
UUID=e06097bb-cfcd-437b-9e4d-a691f5662a7d /store nfs rw,noexec 0 0
```

If a file system found in `/etc/fstab` refers to NFS and it does not have the `noexec` option set, and use of NFS imported binaries is not documented with the Authorizing Official as an operational requirement, refer to the remediation procedure below.

Verify the NFS is mounted with the `noexec` option:

```
# mount | grep nfs | grep noexec
```

If no results are returned and use of NFS imported binaries is not documented with the Authorizing Official as an operational requirement, refer to the remediation procedure below.

Remediation:

Configure the `/etc/fstab` to use the `noexec` option on file systems that are being imported via NFS.

Example: `vim /etc/fstab`

Add, or update any NFS file systems found in the Audit to include the `noexec` option:

```
UUID=e06097bb-cfcd-437b-9e4d-a691f5662a7d /store nfs rw,nosuid,noexec 0 0
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204483
Rule ID: SV-204483r603261_rule
STIG ID: RHEL-07-021021
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

1.1.24 Ensure nosuid option is set for NFS (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 being imported via Network File System (NFS).

Rationale:

The "nosuid" mount option causes the system to not 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 are being NFS imported are configured with the `nosuid` option. Find the file system(s) that contain the directories being exported with the following command:

```
# more /etc/fstab | grep nfs
UUID=e06097bb-cfcd-437b-9e4d-a691f5662a7d /store nfs rw,nosuid 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.

Verify the NFS is mounted with the `nosuid` option:

```
# mount | grep nfs | grep nosuid
```

If no results are returned, refer to the remediation procedure below.

Remediation:

Configure the `/etc/fstab` to use the `nosuid` option on file systems that are being imported via NFS.

Example: `vim /etc/fstab`

Add, uncomment or update the NFS file systems identified in the Audit:

```
UUID=e06097bb-cfcd-437b-9e4d-a691f5662a7d /store nfs rw,nosuid 0 0
```


References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204482
Rule ID: SV-204482r603261_rule
STIG ID: RHEL-07-021020
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

1.1.25 Ensure sticky bit is set on all world-writable directories (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

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:

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 command to verify no world writable directories exist without the sticky bit set:

```
# df --local -P 2> /dev/null | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type d \( -perm -0002 -a ! -perm -1000 \) 2>/dev/null
```

No output should be returned.

Remediation:

Run the following command to set the sticky bit on all world writable directories:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type d \( -perm -0002 -a ! -perm -1000 \) 2>/dev/null | xargs -I '{}' chmod a+t '{}'
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	13 <u>Data Protection</u> Data Protection			

1.1.26 Ensure all world-writable directories are group-owned. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that all world-writable directories are group-owned by root, sys, bin, or an application group.

Rationale:

If a world-writable directory has the sticky bit set and is not group-owned by a privileged 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:

Verify all world-writable directories are group-owned by root, sys, bin, or an application group.

Check the system for world-writable directories with the following command:

Note: The value after -fstype must be replaced with the filesystem type. xfs is used as an example.

```
# find / -xdev -perm -002 -type d -fstype xfs -exec ls -lLd {} \;  
  
drwxrwxrwt 2 root root 40 Aug 26 13:07 /dev/mqueue  
drwxrwxrwt 2 root root 220 Aug 26 13:23 /dev/shm  
drwxrwxrwt 14 root root 4096 Aug 26 13:29 /tmp
```

Review list of the world-writable directories to ensure they are owned by root, sys, bin, or an application group associated with the directory and annotated in the system security plan. If any are discovered not associated correctly refer to the remediation procedure below.

Remediation:

Referring to the list obtained in the Audit above, change the group of the world-writable directories to `root` with the following command:

```
# chgrp root <directory>
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204487
Rule ID: SV-204487r744106_rule
STIG ID: RHEL-07-021030
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

1.1.27 Disable Automounting (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.

Audit:

Run the following command to verify `autofs` is not enabled:

```
# systemctl show "autofs.service" | grep -i unitfilestate=enabled  
Nothing should be returned
```

Remediation:

Run the following command to mask `autofs`:

```
# systemctl --now mask autofs
```

OR run the following command to remove `autofs`

```
# yum remove autofs
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b
5. CCI-000778: The information system uniquely identifies an organization defined list of specific and/or types of devices before establishing a local, remote, or network connection.
6. NIST SP 800-53 :: IA-3
7. NIST SP 800-53A :: IA-3.1 (ii)
8. NIST SP 800-53 Revision 4 :: IA-3
9. CCI-001958: The information system authenticates an organization defined list of specific and/or types of devices before establishing a local, remote, or network connection.
10. NIST SP 800-53 Revision 4 :: IA-3

Additional Information:

- Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.
- 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 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204451
Rule ID: SV-204451r603261_rule
STIG ID: RHEL-07-020110
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.3 <u>Disable Autorun and Autoplay for Removable Media</u> Disable autorun and autoplay auto-execute functionality for removable media.			
v7	8.4 <u>Configure Anti-Malware Scanning of Removable Devices</u> Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.			
v7	8.5 <u>Configure Devices Not To Auto-run Content</u> Configure devices to not auto-run content from removable media.			

1.1.28 Disable USB Storage (Automated)

Profile Applicability:

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

Description:

USB storage provides a means to transfer and store files insuring 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.

Audit:

Run the following commands and verify the output is as indicated:

```
# modprobe -n -v usb-storage  
  
install /bin/true  
# lsmod | grep usb-storage  
  
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

Example: `vim /etc/modprobe.d/usb_storage.conf`

Add the following line:

```
install usb-storage /bin/true
```

Run the following command to unload the usb-storage module:

```
rmmod usb-storage
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b
5. CCI-000778: The information system uniquely identifies an organization defined list of specific and/or types of devices before establishing a local, remote, or network connection.
6. NIST SP 800-53 :: IA-3
7. NIST SP 800-53A :: IA-3.1 (ii)
8. NIST SP 800-53 Revision 4 :: IA-3
9. CCI-001958: The information system authenticates an organization defined list of specific and/or types of devices before establishing a local, remote, or network connection.
10. NIST SP 800-53 Revision 4 :: IA-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 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204449
Rule ID: SV-204449r603261_rule
STIG ID: RHEL-07-020100
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	8.4 <u>Configure Anti-Malware Scanning of Removable Devices</u> Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.			
v7	8.5 <u>Configure Devices Not To Auto-run Content</u> Configure devices to not auto-run content from removable media.			

1.2 Configure Software Updates

Most distributions use a package manager such as yum, apt, or zypper to install and update software packages. 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. Many large enterprises prefer to test patches on a non-production system before rolling out to production.

For the purpose of this benchmark, the requirement is to ensure that a patch management system is configured and maintained. The specifics on patch update procedures are left to the organization.

1.2.1 Ensure GPG keys are configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Most packages managers implement GPG key signing to verify package integrity during 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.

Audit:

Verify GPG keys are configured correctly for your package manager. Depending on the package management in use one of the following command groups may provide the needed information:

```
# rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} --> %{summary}\n'
```

Remediation:

Update your package manager GPG keys in accordance with site policy.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.3 Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v8	<u>7.4 Perform Automated Application Patch Management</u> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<u>3.4 Deploy Automated Operating System Patch Management Tools</u> 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	<u>3.5 Deploy Automated Software Patch Management Tools</u> 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.			

1.2.2 Ensure package manager repositories are configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Systems need to have package manager repositories configured to ensure they 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:

```
# yum repolist
```

Remediation:

Configure your package manager repositories according to site policy.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.3 Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v8	<u>7.4 Perform Automated Application Patch Management</u> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<u>3.4 Deploy Automated Operating System Patch Management Tools</u> 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	<u>3.5 Deploy Automated Software Patch Management Tools</u> 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.			

1.2.3 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/yum.conf` and individual `/etc/yum/repos.d/*.repo` 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:

Run the following command and verify `gpgcheck` is set to 1:

```
# grep ^\s*gpgcheck /etc/yum.conf
gpgcheck=1
```

Run the following command and verify that all instances of `gpgcheck` are set to 1:

```
# grep -P '^h*gpgcheck=[^1\n\r]+\b(\h+.)?$' /etc/yum.conf
/etc/yum/repos.d/*.repo
Nothing should be returned
```

Remediation:

Edit `/etc/yum.conf` and set `'gpgcheck=1'` in the `[main]` section.

Edit any failing files in `/etc/yum/repos.d/*.repo` and set all instances of `gpgcheck` to 1.

References:

1. CCI: CCI-001749: The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.
2. NIST SP 800-53 Revision 4 :: CM-5 (3)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204447
Rule ID: SV-204447r603261_rule
STIG ID: RHEL-07-020050
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.3 Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<u>3.4 Deploy Automated Operating System Patch Management Tools</u> 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.			

1.2.4 Ensure software packages have been digitally signed by a Certificate Authority (CA) (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 of local packages without verification that they have been digitally signed using a certificate that is recognized and approved by the Authorizing Official of the organization.

Check that `yum` verifies the signature of local packages prior to install with the following command:

```
# grep localpkg_gpgcheck /etc/yum.conf  
localpkg_gpgcheck=1
```

If `localpkg_gpgcheck` is not set to 1, or if options are missing or commented out, ask how the signatures of local packages and other operating system components are verified. If there is no process to validate the signatures of local packages that is approved by the organization, refer to the remediation procedure below.

Remediation:

Configure the operating system to verify the signature of local packages prior to install by setting the following option in the `/etc/yum.conf` file:

Example: `vim /etc/yum.conf`
and add the following line:

```
localpkg_gpgcheck=1
```

References:

1. CCI: CCI-001749: The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.
2. NIST SP 800-53 Revision 4 :: CM-5 (3)

Additional Information:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide  
Version 3, Release: 4 Benchmark Date: 23 Jul 2021  
  
Vul ID: V-204448  
Rule ID: SV-204448r603261_rule  
STIG ID: RHEL-07-020060  
Severity: CAT I
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.3 Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v8	<u>7.4 Perform Automated Application Patch Management</u> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<u>3.4 Deploy Automated Operating System Patch Management Tools</u> 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	<u>3.5 Deploy Automated Software Patch Management Tools</u> 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.			

1.2.5 Ensure removal of software components after update (Automated)

Profile Applicability:

- STIG

Description:

The operating system must remove all software components after updated versions have been installed.

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 `yum` is configured to remove unneeded packages with the following command:

```
# grep -i clean_requirements_on_remove /etc/yum.conf  
clean_requirements_on_remove=1
```

If `clean_requirements_on_remove` is not set to 1, True, or yes, or is not set in `/etc/yum.conf`, refer to the remediation procedure below.

Remediation:

Configure the operating system to remove all software components after updated versions have been installed.

Set the `clean_requirements_on_remove` option to 1 in the `/etc/yum.conf` file:

Example: `vim /etc/yum.conf`

Add, uncomment or update the following line:

```
clean_requirements_on_remove=1
```

References:

1. CCI: CCI-002617: The organization removes organization-defined software components (e.g., previous versions) after updated versions have been installed.
2. NIST SP 800-53 Revision 4 :: SI-2 (6)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204452
Rule ID: SV-204452r603261_rule
STIG ID: RHEL-07-020200
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.3 Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v8	<u>7.4 Perform Automated Application Patch Management</u> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<u>3.4 Deploy Automated Operating System Patch Management Tools</u> 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	<u>3.5 Deploy Automated Software Patch Management Tools</u> 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.			

1.2.6 Ensure the version of the operating system is an active vendor supported release (Manual)

Profile Applicability:

- STIG

Description:

The operating system must be a vendor supported release

Rationale:

An operating system release is considered "supported" if the vendor continues to provide security patches for the product. With an unsupported release, it will not be possible to resolve security issues discovered in the system software.

Red Hat offers the Extended Update Support (EUS) Add-On to a Red Hat Enterprise Linux subscription, for a fee, for those customers who wish to standardize on a specific minor release for an extended period. RHEL 7.7 marks the final minor release that EUS will be available, while 7.9 is the final minor release overall.

Audit:

Verify the version of the operating system is vendor supported.

Check the version of the operating system with the following command:

```
# cat /etc/redhat-release  
Red Hat Enterprise Linux Server release 7.9 (Maipo)
```

Current End of Extended Update Support for RHEL 7.6 is 31 May 2021.

Current End of Extended Update Support for RHEL 7.7 is 30 August 2021.

Current End of Maintenance Support for RHEL 7.9 is 30 June 2024.

If the release is not supported by the vendor, this is a finding.

Remediation:

Upgrade to a supported version of the operating system.

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204458
Rule ID: SV-204458r744100_rule
STIG ID: RHEL-07-020250
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>2.2 Ensure Authorized Software is Currently Supported</u> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			
v7	<u>2.2 Ensure Software is Supported by Vendor</u> Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.			

1.3 Filesystem Integrity Checking

AIDE is a file integrity checking tool, similar in nature to Tripwire. 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.

1.3.1 Ensure AIDE is installed (Automated)

Profile Applicability:

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

Description:

AIDE takes a snapshot of filesystem state 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.

Note: 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.

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:

```
# yum 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. CCI: CCI-001744: The information system implements organization-defined security responses automatically if baseline configurations are changed in an unauthorized manner.
3. NIST SP 800-53 Revision 4 :: CM-3 (5)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204445
Rule ID: SV-204445r603261_rule
STIG ID: RHEL-07-020030
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 <u>Log Sensitive Data Access</u> Log sensitive data access, including modification and disposal.			●
v7	14.9 <u>Enforce Detail Logging for Access or Changes to Sensitive Data</u> 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).			●

1.3.2 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.

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 aidcheck.service and aidcheck.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. CCI: CCI-001744: The information system implements organization-defined security responses automatically if baseline configurations are changed in an unauthorized manner.
4. NIST SP 800-53 Revision 4 :: 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 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204445
Rule ID: SV-204445r603261_rule
STIG ID: RHEL-07-020030
Severity: CAT II

Vul ID: V-204446
Rule ID: SV-204446r603261_rule
STIG ID: RHEL-07-020040
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 <u>Log Sensitive Data Access</u> Log sensitive data access, including modification and disposal.			●
v7	14.9 <u>Enforce Detail Logging for Access or Changes to Sensitive Data</u> 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).			●

1.3.3 Ensure AIDE is configured to verify ACLs (Manual)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that the file integrity tool is 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.

Audit:

Verify the file integrity tool is configured to verify ACLs.

Note: AIDE is highly configurable at install time. These commands assume 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 `acl` rule has been added to the rule list being applied to the files and directories selection lists.

An example rule that includes the `acl` rule is below:

```
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 `acl` rule is not being used on all uncommented selection lines in the `/etc/aide.conf` file, or ACLs are not being checked by another file integrity tool, refer to the remediation procedure below.

Remediation:

Configure the file integrity tool to check file and directory ACLs.

If AIDE is installed, ensure the `acl` rule is present on all uncommented file and directory selection lists.

Example: `vim /etc/aide.conf`

add a rule that includes the `acl` example:

```
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
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

This checks for `aide.conf` in the default location. If `aide.conf` is in a different location, manually confirm that the setting(s) are correct.

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204498
Rule ID: SV-204498r603261_rule
STIG ID: RHEL-07-021600
Severity: CAT III
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

1.3.4 Ensure AIDE is configured to verify XATTRS (Manual)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that the file integrity tool is configured to verify extended attributes.

Rationale:

Extended attributes in file systems are used to contain arbitrary data and file metadata with security implications.

Audit:

Verify the file integrity tool is configured to verify extended attributes.

Note: AIDE is highly configurable at install time. These commands assume 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, refer to the remediation procedure below.

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.

Example: `vim /etc/aide.conf`

add rule that includes the `xattrs` example:

```
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
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204499
Rule ID: SV-204499r603261_rule
STIG ID: RHEL-07-021610
Severity: CAT III
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

1.3.5 Ensure AIDE is configured to use FIPS 140-2 (Manual)

Profile Applicability:

- STIG

Description:

The operating system must use a file integrity tool that is configured to use FIPS 140-2 approved cryptographic hashes for validating file contents and directories.

Rationale:

File integrity tools use cryptographic hashes for verifying file contents and directories have not been altered. These hashes must be FIPS 140-2 approved cryptographic hashes.

Audit:

Verify the file integrity tool is configured to use FIPS 140-2 approved cryptographic hashes for validating file contents and directories.

Note: AIDE is highly configurable at install time. These commands assume 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 `sha512` rule has been added to the rule list being applied to the files and directories selection lists.

An example rule that includes the `sha512` 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 `sha512` rule is not being used on all uncommented selection lines in the `/etc/aide.conf` file, or another file integrity tool is not using FIPS 140-2 approved cryptographic hashes for validating file contents and directories, refer to the remediation procedure below.

Remediation:

Configure the file integrity tool to use FIPS 140-2 cryptographic hashes for validating file and directory contents.

If AIDE is installed, ensure the `sha512` rule is present on all uncommented file and directory selection lists.

Example: `vim /etc/aide.conf`

add a rule that includes the `sha512` example:

```
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
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204500
Rule ID: SV-204500r603261_rule
STIG ID: RHEL-07-021620
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

1.4 Secure Boot Settings

The recommendations in this section focus on securing the bootloader and settings involved in the boot process directly.

1.4.1 Ensure bootloader password is set (Automated)

Profile Applicability:

- 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
- You can add --unrestricted to the menu entries to allow the system to boot without entering a password. Password will still be required to edit menu items.

Audit:

Run the following script to verify the bootloader password has been set:

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

GBPC()
{
    tst1="" tst2="" output=""
    grubfile=$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o -
name 'grub.cfg' \) -exec grep -El '^s*(kernelopts=|linux|kernel)' {} \;)
    grubdir=$(dirname "$grubfile")
    userfile="$grubdir/user.cfg"

    if [ -f "$userfile" ]; then
        grep -Pq '^h*GRUB2_PASSWORDh*=\h*.\+$' "$userfile" &&
output="bootloader password set in \"$userfile\""
    fi
    if [ -z "$output" ]; then
        grep -Piq '^h*seth+superusersh*=\h*"?"[^"\n\r]+"?(\h+.)?$(
"$grubfile" && tst1=pass
        grep -Piq '^h*password(_pbkdf2)?\h+\H\h+.\+$' "$grubfile" && tst2=pass
        [ "$tst1" = pass ] && [ "$tst2" = pass ] && output="bootloader password
set in \"$grubfile\""
    fi
    [ -n "$output" ] && echo -e "\n\n PASSED! $output\n\n"
}
GBPC
```

Remediation:

For newer grub2 based systems (Release 7.2 and newer), create an encrypted password with grub2-setpassword:

```
# grub2-setpassword

Enter password: <password>
Confirm password: <password>
```

Run the following command to script the grub2 configuration:

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

GFCU()
{
    grubfile=$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o -
name 'grub.cfg' \) -exec grep -Pl '^h*(kernelopts=|linux|kernel)' {} \;)
    grubdir=$(dirname "$grubfile")
    grub2-mkconfig -o "$grubdir/grub.cfg"
}
GFCU
```


OR for older grub2 based systems, create an encrypted password with `grub2-mkpasswd-pbkdf2`:

```
# grub2-mkpasswd-pbkdf2

Enter password: <password>
Reenter password: <password>

Your PBKDF2 is <encrypted-password>
```

Add the following into `/etc/grub.d/01_users` or a custom `/etc/grub.d` configuration file:

```
cat <<EOF
set superusers="<username>"
password_pbkdf2 <username> <encrypted-password>
EOF
```

Note:

- *If placing the information in a custom file, do not include the "cat << EOF" and "EOF" lines as the content is automatically added from these files*
- *The superuser/user information and password should not be contained in the `/etc/grub.d/00_header` file. The information can be placed in any `/etc/grub.d` file as long as that file is incorporated into `grub.cfg`. It is preferable to enter this data into a custom file, such as `/etc/grub.d/40_custom`, so it is not overwritten should the Grub package be updated*

Run the following command to script the grub2 configuration:

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

GFCU()
{
    grubfile=$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o -
name 'grub.cfg' \) -exec grep -Pl '^h*(kernelopts=|linux|kernel)' {} \;)
    grubdir=$(dirname "$grubfile")
    grub2-mkconfig -o "$grubdir/grub.cfg"
}

GFCU
```

References:

1. CCI: CCI-000213: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
2. NIST SP 800-53 :: AC-3
3. NIST SP 800-53A :: AC-3.1
4. NIST SP 800-53 Revision 4 :: AC-3

Additional Information:

The `older` method will also work on Release 7.2 and newer systems

This recommendation is designed around the grub2 bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings. Replace `/boot/grub2/grub.cfg` with the appropriate grub configuration file for your environment

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204436
Rule ID: SV-204436r603261_rule
STIG ID: RHEL-07-010480
Severity: CAT I

Vul ID: V-204438
Rule ID: SV-204438r744095_rule
STIG ID: RHEL-07-010482
Severity: CAT I

Vul ID: V-204439
Rule ID: SV-204439r603261_rule
STIG ID: RHEL-07-010490
Severity: CAT I

Vul ID: V-204440
Rule ID: SV-204440r744098_rule
STIG ID: RHEL-07-010491
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process 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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.4.2 Ensure permissions on bootloader config are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The grub configuration file contains information on boot settings and passwords for unlocking boot options. The grub2 configuration is usually `grub.cfg`. On newer grub2 systems the encrypted bootloader password is contained in `user.cfg`.

If the system uses UEFI, `/boot/efi` is a vfat filesystem. The vfat filesystem itself doesn't have the concept of permissions but can be mounted under Linux with whatever permissions desired.

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 correct permissions, ownership, and group for the grub files:

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

GFPT()
{
    tst1="" tst2="" tst3="" tst4="" tst5="" tst6="" output="" output2=""
    output3="" output4="" output5="" output6=""
    grubfile=$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o -
name 'grub.cfg' \) -exec grep -Pl '^h*(kernelopts=|linux|kernel)' {} \;)
    grubdir=$(dirname "$grubfile")
    stat -c "%a" "$grubfile" | grep -Pq '^h*[0-7]00$' && tst1=pass
    output="Permissions on \"$grubfile\" are \"$(stat -c "%a" "$grubfile")\""
    stat -c "%u:%g" "$grubfile" | grep -Pq '^h*0:0$' && tst2=pass
    output2="\"$grubfile\" is owned by \"$(stat -c "%U" "$grubfile")\" and
belongs to group \"$(stat -c "%G" "$grubfile")\""
    if [ -f "$grubdir/user.cfg" ]; then
        stat -c "%a" "$grubdir/user.cfg" | grep -Pq '^h*[0-7]00$' && tst3=pass
        output3="Permissions on \"$grubdir/user.cfg\" are \"$(stat -c "%a"
"$grubdir/user.cfg")\""
        stat -c "%u:%g" "$grubdir/user.cfg" | grep -Pq '^h*0:0$' && tst4=pass
        output4="\"$grubdir/user.cfg\" is owned by \"$(stat -c "%U"
"$grubdir/user.cfg")\" and belongs to group \"$(stat -c "%G"
"$grubdir/user.cfg")\""
    else
        tst3=pass;tst4=pass
    fi
    if [ -f "$grubdir/grub.cfg" ]; then
        stat -c "%a" "$grubdir/grub.cfg" | grep -Pq '^h*[0-7]00$' && tst5=pass
        output5="Permissions on \"$grubdir/grub.cfg\" are \"$(stat -c "%a"
"$grubdir/grub.cfg")\""
        stat -c "%u:%g" "$grubdir/grub.cfg" | grep -Pq '^h*0:0$' && tst6=pass
        output6="\"$grubdir/grub.cfg\" is owned by \"$(stat -c "%U"
"$grubdir/grub.cfg")\" and belongs to group \"$(stat -c "%G"
"$grubdir/grub.cfg")\""
    else
        tst5=pass;tst6=pass
    fi
    if [ "$tst1" = "pass" ] && [ "$tst2" = "pass" ] && [ "$tst3" = "pass" ] &&
[ "$tst4" = "pass" ] && [ "$tst5" = "pass" ] && [ "$tst6" = "pass" ]; then
        echo "PASSED: "
    else
        echo "FAILED: "
    fi
    [ -n "$output" ] && echo "$output";[ -n "$output2" ] && echo "$output2";[
-n "$output3" ] && echo "$output3"
    [ -n "$output4" ] && echo "$output4";[ -n "$output5" ] && echo
"$output5";[ -n "$output6" ] && echo "$output6"
}
GFPT
```

Remediation:

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 og-rwx /boot/grub2/grub.cfg

# [ -f /boot/grub2/user.cfg ] && chown root:root /boot/grub2/user.cfg
# [ -f /boot/grub2/user.cfg ] && chmod og-rwx /boot/grub2/user.cfg
```

OR If the system uses UEFI, edit `/etc/fstab` and add the `fmask=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

Additional Information:

This recommendation is designed around the grub2 bootloader.

If LILO or another bootloader is in use in your environment:

- Enact equivalent settings
- Replace `/boot/grub2/grub.cfg` and `/boot/grub2/user.cfg` with the appropriate boot configuration files for your environment

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.4.3 Ensure authentication required for single user mode (Automated)

Profile Applicability:

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

Description:

Single user mode (rescue mode) is used for recovery when the system detects an issue during boot or by manual selection from the bootloader.

Note: The systemctl option --fail is synonymous with --job-mode=fail. Using either is acceptable.

Rationale:

Requiring authentication in single user mode (rescue mode) prevents an unauthorized user from rebooting the system into single user to gain root privileges without credentials.

Audit:

Run the following commands and verify that `/sbin/sulogin` or `/usr/sbin/sulogin` is used as shown:

```
# grep /sbin/sulogin /usr/lib/systemd/system/rescue.service
ExecStart=/bin/sh -c "/sbin/sulogin; /usr/bin/systemctl --fail --no-block
default"
# grep /sbin/sulogin /usr/lib/systemd/system/emergency.service
ExecStart=/bin/sh -c "/sbin/sulogin; /usr/bin/systemctl --fail --no-block
default"
```

Remediation:

Edit `/usr/lib/systemd/system/rescue.service` and `/usr/lib/systemd/system/emergency.service` and set `ExecStart` to use `/sbin/sulogin` or `/usr/sbin/sulogin`:

```
ExecStart=/bin/sh -c "/sbin/sulogin; /usr/bin/systemctl --fail --no-block
default"
```

References:

1. CCI: CCI-000213: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
2. NIST SP 800-53 :: AC-3
3. NIST SP 800-53A :: AC-3.1
4. NIST SP 800-53 Revision 4 :: AC-3

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204437
Rule ID: SV-204437r603261_rule
STIG ID: RHEL-07-010481
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.4.4 Ensure boot loader does not allow removable media (Automated)

Profile Applicability:

- STIG

Description:

The operating system must not allow removable media to be used as the boot loader unless approved.

Rationale:

Malicious users with removable boot media can gain access to a system configured to use removable media as the boot loader. If removable media is designed to be used as the boot loader, the requirement must be documented with the Information System Security Officer (ISSO).

Audit:

Verify the system is not configured to use a boot loader on removable media.

Note: GRUB 2 reads its configuration from the `/boot/grub2/grub.cfg` file on traditional BIOS-based machines and from the `/boot/efi/EFI/redhat/grub.cfg` file on UEFI machines.

Check for the existence of alternate boot loader configuration files with the following command:

```
# find / -name grub.cfg
/boot/grub2/grub.cfg
```

If a `grub.cfg` is found in any subdirectories other than `/boot/grub2` and `/boot/efi/EFI/redhat`, ask the Authorizing Official if there is documentation signed to approve the use of removable media as a boot loader.

Check that the grub configuration file has the `set root` command in each menu entry with the following commands:

```
# grep -c menuentry /boot/grub2/grub.cfg
1
# grep 'set root' /boot/grub2/grub.cfg
set root=(hd0,1)
```


If the system is using an alternate boot loader on removable media, and documentation does not exist approving the alternate configuration, refer to the remediation procedure below.

Remediation:

Remove alternate methods of booting the system from removable media or document the configuration to boot from removable media with the Authorizing Official.

Example: `vim /etc/default/grub`

Add this in the first menu entry

```
set root=(hd0,1)
```

Any changes made to `/etc/default/grub` require you to run `grub2-mkconfig` to re-generate the `/boot/grub2/grub.cfg` file.

Example:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

References:

1. CCI-000318: The organization audits and reviews activities associated with configuration controlled changes to the system.
2. NIST SP 800-53 :: CM-3 e
3. NIST SP 800-53A :: CM-3.1 (v)
4. NIST SP 800-53 Revision 4 :: CM-3 f
5. CCI-000368: The organization documents any deviations from the established configuration settings for organization-defined information system components based on organization-defined operational requirements.
6. NIST SP 800-53 :: CM-6 c
7. NIST SP 800-53A :: CM-6.1 (v)
8. NIST SP 800-53 Revision 4 :: CM-6 c
9. CCI-001812: The information system prohibits user installation of software without explicit privileged status.
10. NIST SP 800-53 Revision 4 :: CM-11 (2)
11. CCI-001813: The information system enforces access restrictions.
12. NIST SP 800-53 Revision 4 :: CM-5 (1)
13. CCI-001814: The Information system supports auditing of the enforcement actions.
14. NIST SP 800-53 Revision 4 :: CM-5 (1)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204501
Rule ID: SV-204501r603261_rule
STIG ID: RHEL-07-021700
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.4.5 Ensure version 7.2 or newer booted with a BIOS have a unique name for the grub superusers account (Manual)

Profile Applicability:

- STIG

Description:

The Linux operating systems version 7.2 or newer booted with a BIOS must have a unique name for the grub superusers account when 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 7 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.

For systems that are running a version of RHEL prior to 7.2, 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 /boot/grub2/grub.cfg file and add or modify the following lines in the "### BEGIN /etc/grub.d/01_users ###" section:

```
set superusers="[someuniquestringhere]"  
export superusers  
password_pbkdf2 [someuniquestringhere] ${GRUB2_PASSWORD}
```

References:

1. CCI-000213: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies
2. NIST SP 800-53 :: AC-3
3. NIST SP 800-53A :: AC-3.1
4. NIST SP 800-53 Revision 4 :: AC-3

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-244557
Rule ID: SV-244557r744063_rule
STIG ID: RHEL-07-010483
Severity: CAT II

1.4.6 Ensure version 7.2 or newer booted with UEFI have a unique name for the grub superusers account (Manual)

Profile Applicability:

- STIG

Description:

The Linux operating systems version 7.2 or newer booted with United Extensible Firmware Interface (UEFI) must have a unique name for the grub superusers account when 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 7 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.

For systems that are running a version of RHEL prior to 7.2, 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 /boot/efi/EFI/redhat/grub.cfg file and add or modify the following lines in the "### BEGIN /etc/grub.d/01_users ###" section:

```
set superusers="[someuniquestringhere]"  
export superusers  
password_pbkdf2 [someuniquestringhere] ${GRUB2_PASSWORD}
```

References:

1. CCI-000213: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies
2. NIST SP 800-53 :: AC-3
3. NIST SP 800-53A :: AC-3.1
4. NIST SP 800-53 Revision 4 :: AC-3

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-244558
Rule ID: SV-244558r744066_rule
STIG ID: RHEL-07-010492
Severity: CAT II

1.5 Additional Process Hardening

1.5.1 Ensure core dumps are restricted (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. The system provides the ability to set a soft limit for core dumps, but this can be overridden by the user.

Rationale:

Setting a hard limit on core dumps prevents users from overriding the soft variable. If core dumps are required, consider setting limits for user groups (see `limits.conf(5)`). In addition, setting the `fs.suid_dumpable` variable to 0 will prevent setuid programs from dumping core.

Audit:

Run the following commands and verify output matches:

```
# grep -E "^s*\s+hard\s+core" /etc/security/limits.conf
/etc/security/limits.d/*

* hard core 0
# sysctl fs.suid_dumpable

fs.suid_dumpable = 0
# grep "fs\.suid_dumpable" /etc/sysctl.conf /etc/sysctl.d/*

fs.suid_dumpable = 0
```

Run the following command to check if systemd-coredump is installed:

```
# systemctl is-enabled coredump.service
```

If `enabled` or `disabled` is returned systemd-coredump is installed

Remediation:

Add the following line to `/etc/security/limits.conf` or a `/etc/security/limits.d/*` file:

```
* hard core 0
```

Set the following parameter in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
fs.suid_dumpable = 0
```

Run the following command to set the active kernel parameter:

```
# sysctl -w fs.suid_dumpable=0
```

If systemd-coredump is installed:

edit `/etc/systemd/coredump.conf` and add/modify the following lines:

```
Storage=none  
ProcessSizeMax=0
```

Run the command:

```
systemctl daemon-reload
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.5.2 Ensure XD/NX support is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Recent processors in the x86 family support the ability to prevent code execution on a per memory page basis. Generically and on AMD processors, this ability is called No Execute (NX), while on Intel processors it is called Execute Disable (XD). This ability can help prevent exploitation of buffer overflow vulnerabilities and should be activated whenever possible. Extra steps must be taken to ensure that this protection is enabled, particularly on 32-bit x86 systems. Other processors, such as Itanium and POWER, have included such support since inception and the standard kernel for those platforms supports the feature.

Rationale:

Enabling any feature that can protect against buffer overflow attacks enhances the security of the system.

Note: Ensure your system supports the XD or NX bit and has PAE support before implementing this recommendation as this may prevent it from booting if these are not supported by your hardware.

Audit:

Run the following command and verify your kernel has identified and activated NX/XD protection.

```
# journalctl | grep 'protection: active'

kernel: NX (Execute Disable) protection: active
```

OR

on systems without journalctl:

```
# [[ -n $(grep noexec[0-9]*=off /proc/cmdline) || -z $(grep -E -i ' (pae|nx)' /proc/cpuinfo) || -n $(grep '\sNX\s.*\sprotection:\s' /var/log/dmesg | grep -v active) ]] && echo "NX Protection is not active"

Nothing should be returned
```

Remediation:

On 32 bit systems install a kernel with PAE support, no installation is required on 64 bit systems:

If necessary configure your bootloader to load the new kernel and reboot the system.

You may need to enable NX or XD support in your bios.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> 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	8.3 <u>Enable Operating System Anti-Exploitation Features/</u> <u>Deploy Anti-Exploit Technologies</u> 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.			

1.5.3 Ensure address space layout randomization (ASLR) 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 commands and verify output matches:

```
# sysctl kernel.randomize_va_space  
  
kernel.randomize_va_space = 2  
# grep "kernel\.randomize_va_space" /etc/sysctl.conf /etc/sysctl.d/*  
  
kernel.randomize_va_space = 2
```

Remediation:

Set the following parameter in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
kernel.randomize_va_space = 2
```

Run the following command to set the active kernel parameter:

```
# sysctl -w kernel.randomize_va_space=2
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204584
Rule ID: SV-204584r603261_rule
STIG ID: RHEL-07-040201
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> 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	8.3 <u>Enable Operating System Anti-Exploitation Features/Deploy Anti-Exploit Technologies</u> 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.			

1.5.4 Ensure prelink is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`prelink` is a program that modifies ELF shared libraries and ELF dynamically linked binaries in such a way that the time needed for the dynamic linker to perform relocations at startup significantly decreases.

Rationale:

The prelinking feature can interfere with the operation of AIDE, because it changes binaries. Prelinking can also increase the vulnerability of the system if a malicious user is able to compromise a common library such as `libc`.

Audit:

Verify `prelink` is not installed.

Run the following command:

```
# rpm -q prelink
package prelink is not installed
```

Remediation:

Run the following command to restore binaries to normal:

```
# prelink -ua
```

Run the following command to uninstall `prelink`:

```
# yum remove prelink
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>14.9 Enforce Detail Logging for Access or Changes to Sensitive Data</u> 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).			

1.5.5 Ensure number of concurrent sessions is limited (Automated)

Profile Applicability:

- STIG

Description:

The operating system must limit the number of concurrent sessions to 10 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 "maxlogins" /etc/security/limits.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 not set to 10 or less for all domains that have the `maxlogins` item assigned, refer to the remediation procedure below.

Remediation:

Configure the operating system to limit the number of concurrent sessions to 10 for all accounts and/or account types.

Example: `vim /etc/security/limits.conf`

Add the following line to the top of the `/etc/security/limits.conf`:

```
* hard maxlogins 10
```


References:

1. CCI-000054: The information system limits the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number of sessions
2. NIST SP 800-53 :: AC-10
3. NIST SP 800-53A :: AC-10.1 (ii)
4. NIST SP 800-53 Revision 4 :: AC-10

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204576
Rule ID: SV-204576r603261_rule
STIG ID: RHEL-07-040000
Severity: CAT III

1.5.6 Ensure the Ctrl-Alt-Delete key sequence is disabled. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that the user will be prompted when Ctrl-Alt-Delete key sequence is entered.

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 the GNOME graphical 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.

Check that the `ctrl-alt-del.target` is masked and not active with the following command:

```
# systemctl status ctrl-alt-del.target

ctrl-alt-del.target
Loaded: masked (/dev/null; bad)
Active: inactive (dead)
```

If the `ctrl-alt-del.target` is not masked, or if the `ctrl-alt-del.target` is active, refer to the remediation procedure below.

Remediation:

Configure the system to disable the `Ctrl-Alt_Delete` sequence for the command line with the following command:

```
# systemctl mask ctrl-alt-del.target
```

If GNOME is active on the system, create a database to contain the system-wide setting (if it does not already exist) with the following command:

```
# touch /etc/dconf/db/local.d/00-disable-CAD
```

Add the setting to disable the `Ctrl-Alt_Delete` sequence for GNOME:

```
[org/gnome/settings-daemon/plugins/media-keys]
logout=''
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204455
Rule ID: SV-204455r603261_rule
STIG ID: RHEL-07-020230
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.5.7 Ensure kernel core dumps are disabled. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must disable Kernel core 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.

Audit:

Verify that kernel core dumps are disabled unless needed.

Check the status of the `kdump` service with the following command:

```
# systemctl status kdump.service

kdump.service - Crash recovery kernel arming
Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled)
Active: active (exited) since Wed 2015-08-26 13:08:09 EDT; 43min ago
Main PID: 1130 (code=exited, status=0/SUCCESS)
kernel arming.
```

If the `kdump` service is active, the use of the service must be documented with the Authorizing Official.

If the service is active and is not documented, refer to the remediation procedure below.

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 Authorizing Official.

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204492
Rule ID: SV-204492r603261_rule
STIG ID: RHEL-07-021300
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.5.8 Ensure DNS is servers are configured (Automated)

Profile Applicability:

- STIG

Description:

The operating systems that are using DNS resolution, must have at least two name servers 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, refer to the remediation procedure below.

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, refer to the remediation procedure below.

Remediation:

Configure the operating system to use two or more name servers for DNS resolution.

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
```

And then make the file immutable with the following command:

```
# chattr +i /etc/resolv.conf
```

If the `/etc/resolv.conf` file must be mutable, the required configuration must be documented with the Authorizing Official and the file must be verified by the system file integrity tool.

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204608
Rule ID: SV-204608r603261_rule
STIG ID: RHEL-07-040600
Severity: CAT III

1.5.9 Ensure NIST FIPS-validated cryptography is configured (Automated)

Profile Applicability:

- STIG

Description:

The operating system must implement NIST FIPS-validated cryptography for the following:

- provision digital signatures
- generate cryptographic hashes
- protect data requiring data-at-rest protections in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

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.

Audit:

Verify the operating system implements DoD-approved encryption to protect the confidentiality of remote access sessions.

Check to see if the `dracut-fips` package is installed with the following command:

```
# yum list installed dracut-fips  
  
dracut-fips-033-360.el7_2.x86_64.rpm
```

If a `dracut-fips` package is installed, check to see if the kernel command line is configured to use FIPS mode with the following command:

Note: GRUB 2 reads its configuration from the `/boot/grub2/grub.cfg` file on traditional BIOS-based machines and from the `/boot/efi/EFI/redhat/grub.cfg` file on UEFI machines.

```
# grep fips /boot/grub2/grub.cfg  
/vmlinuz-3.8.0-0.40.el7.x86_64 root=/dev/mapper/rhel-root ro rd.md=0 rd.dm=0  
rd.lvm.lv=rhel/swap crashkernel=auto rd.luks=0 vconsole.keymap=us  
rd.lvm.lv=rhel/root rhgb fips=1 quiet
```

If the kernel command line is configured to use FIPS mode, check to see if the system is in FIPS mode with the following command:

```
# cat /proc/sys/crypto/fips_enabled
1
```

If a `dracut-fips` package is not installed, the kernel command line does not have a FIPS entry, or the system has a value of 0 for `fips_enabled` in `/proc/sys/crypto`, refer to the remediation procedure below.

Remediation:

Configure the operating system to implement DoD-approved encryption by installing the `dracut-fips` package.

To enable strict FIPS compliance, the `fips=1` kernel option needs to be added to the kernel command line during system installation so key generation is done with FIPS- approved algorithms and continuous monitoring tests in place.

Configure the operating system to implement DoD-approved encryption by following the steps below:

The `fips=1` kernel option needs to be added to the kernel command line during system installation so that key generation is done with FIPS-approved algorithms and continuous monitoring tests in place. Users should also ensure that 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 non-unique key.

Install the `dracut-fips` package with the following command:

```
# yum install dracut-fips
```

Recreate the `initramfs` file with the following command:

Note: This command will overwrite the existing `initramfs` file.

```
# dracut -f
```

Modify the kernel command line of the current kernel in the `grub.cfg` file by adding the following option to the `GRUB_CMDLINE_LINUX` key in the `/etc/default/grub` file and then rebuild the `grub.cfg` file:

```
fips=1
```

Changes to `/etc/default/grub` require rebuilding the `grub.cfg` file as follows:

On BIOS-based machines, use the following command:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

On UEFI-based machines, use the following command:

```
# grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
```

If `/boot` or `/boot/efi` reside on separate partitions, the kernel parameter `boot=<partition of /boot or /boot/efi>` must be added to the kernel command line. You can identify a partition by running the `df /boot` or `df /boot/efi` command:

```
# df /boot
Filesystem 1K-blocks Used Available Use% Mounted on
/dev/sda1 495844 53780 416464 12% /boot
```

To ensure the `boot=` configuration option will work even if device naming changes occur between boots, identify the universally unique identifier (UUID) of the partition with the following command:

```
# blkid /dev/sda1
/dev/sda1: UUID="05c000f1-a213-759e-c7a2-f11b7424c797" TYPE="ext4"
```

For the example above, append the following string to the kernel command line:

```
boot=UUID=05c000f1-a213-759e-c7a2-f11b7424c797
```

Reboot the system for the changes to take effect.

References:

1. CCI: CCI-000068: The information system implements cryptographic mechanisms to protect the confidentiality of remote access sessions.
2. NIST SP 800-53 :: AC-17 (2)
3. NIST SP 800-53A :: AC-17 (2).1
4. NIST SP 800-53 Revision 4 :: AC-17 (2)
5. CCI-001199: The information system protects the confidentiality and/or integrity of organization-defined information at rest.
6. NIST SP 800-53 :: SC-28
7. NIST SP 800-53A :: SC-28.1
8. NIST SP 800-53 Revision 4 :: SC-28
9. CCI-002450: The information system implements organization-defined cryptographic uses and type of cryptography required for each use in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
10. NIST SP 800-53 Revision 4 :: SC-13
11. CCI-002476: The information system implements cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined information system components.
12. NIST SP 800-53 Revision 4 :: SC-28 (1)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204497
Rule ID: SV-204497r603261_rule
STIG ID: RHEL-07-021350
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> 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> Encrypt all sensitive information in transit.			
v7	18.5 <u>Use Only Standardized and Extensively Reviewed Encryption Algorithms</u> Use only standardized and extensively reviewed encryption algorithms.			

1.6 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.

1.6.1 Configure SELinux

SELinux provides a Mandatory Access Control (MAC) system that greatly augments the default Discretionary Access Control (DAC) model. Under SELinux, every process and every object (files, sockets, pipes) on the system is assigned a security context, a label that includes detailed type information about the object. The kernel allows processes to access objects only if that access is explicitly allowed by the policy in effect. The policy defines transitions, so that a user can be allowed to run software, but the software can run under a different context than the user's default. 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. Three such policies have been designed for use with RHEL7 and are included with the system: `targeted`, `strict`, and `mls`. These are described as follows:

- `targeted`: consists mostly of Type Enforcement (TE) rules, and a small number of Role-Based Access Control (RBAC) rules. Targeted restricts the actions of many types of programs, but leaves interactive users largely unaffected.
- `strict`: also uses TE and RBAC rules, but on more programs and more aggressively.
- `mls`: implements Multi-Level Security (MLS), which introduces even more kinds of labels (sensitivity and category) and rules that govern access based on these.

Notes:

- *This section provides guidance for the configuration of the `targeted` policy.*
- *This section **only** applies if SELinux is in use on the system.*
- *Additional Mandatory Access Control systems exist. If a different MAC is used, such as AppArmor, configure the MAC according to its security guidance.*

References:

- NSA SELinux resources:
 - <http://www.nsa.gov/research/selinux>
 - <http://www.nsa.gov/research/selinux/list.shtml>
- Fedora SELinux resources:
 - FAQ: <http://docs.fedoraproject.org/selinux-faq>
 - User Guide: <http://docs.fedoraproject.org/selinux-user-guide>
 - Managing Services Guide: <http://docs.fedoraproject.org/selinux-managing-confined-services-guide>
- SELinux Project web page and wiki:
 - <http://www.selinuxproject.org>
- Chapters 43-45 of Red Hat Enterprise Linux 5: Deployment Guide (Frank Mayer, Karl MacMillan and David Caplan),
- SELinux by Example: Using Security Enhanced Linux (Prentice Hall, August 6, 2006)

1.6.1.1 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:

```
# yum install libselinux
```


CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>14.6 Protect Information through Access Control Lists</u> 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.			

1.6.1.2 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.

Note: This recommendation is designed around the grub 2 bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

Rationale:

SELinux must be enabled at boot time in your grub configuration to ensure that the controls it provides are not overridden.

Audit:

Run the following command to verify that the `selinux=0` or `enforcing=0` parameters isn't set:

```
# grep -P -- '^h*(kernelopts=|linux|kernel)' $(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg' \) -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;) | grep -E -- '(selinux=0|enforcing=0)'
```

Nothing should be returned

Remediation:

Edit `/etc/default/grub` and remove all instances of `selinux=0` and `enforcing=0` from all `CMDLINE_LINUX` parameters:

```
GRUB_CMDLINE_LINUX_DEFAULT="quiet"

GRUB_CMDLINE_LINUX=""
```

Run the following script to update the `grub2` configuration:

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

GFCU()
{
    grubfile=$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o -
name 'grub.cfg' \) -exec grep -Pl '^\\h*(kernelopts=|linux|kernel)' {} \;)
    grubdir=$(dirname "$grubfile")
    grub2-mkconfig -o "$grubdir/grub.cfg"
}
GFCU
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

1.6.1.3 Ensure SELinux policy is configured (Automated)

Profile Applicability:

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

Description:

Configure SELinux to meet or exceed the default targeted policy, which constrains daemons and system software only.

Note: If your organization requires stricter policies, ensure that they are set in the `/etc/selinux/config` file.

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 SELINUXTYPE= /etc/selinux/config
SELINUXTYPE=targeted
# sestatus | grep 'Loaded policy'
Loaded policy name:          targeted
```

Remediation:

Edit the `/etc/selinux/config` file to set the SELINUXTYPE parameter:

```
SELINUXTYPE=targeted
```

References:

1. CCI: CCI-002165: The information system enforces organization-defined discretionary access control policies over defined subjects and objects.
2. NIST SP 800-53 Revision 4 :: AC-3 (4)
3. CCI-002696: The information system verifies correct operation of organization-defined security functions.
4. NIST SP 800-53 Revision 4 :: SI-6 a

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204454
Rule ID: SV-204454r754748_rule
STIG ID: RHEL-07-020220
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

1.6.1.4 Ensure the SELinux mode is enforcing or permissive (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 commands and ensure output matches:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

1.6.1.5 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.

Audit:

Run the following commands and ensure output matches:

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
2. CCI: 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

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204453
Rule ID: SV-204453r754746_rule
STIG ID: RHEL-07-020210
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

1.6.1.6 Ensure no unconfined services exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Unconfined processes run in unconfined domains

Note: 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.

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

Audit:

Run the following command and verify not output is produced:

```
# ps -eZ | grep unconfined_service_t
```

Remediation:

Investigate any unconfined processes found during the audit action. They may need to have an existing security context assigned to them or a policy built for them.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

1.6.1.7 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`:

```
# yum remove setroubleshoot
```

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> 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>14.6 Protect Information through Access Control Lists</u> 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.			

1.6.1.8 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:

Verify `mcstrans` is not installed.

Run the following command:

```
# rpm -q mcstrans  
package mcstrans is not installed
```

Remediation:

Run the following command to uninstall `mcstrans`:

```
# yum remove mcstrans
```


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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

1.6.1.9 Ensure non-privileged users are prevented from executing privileged functions (Manual)

Profile Applicability:

- STIG

Description:

The operating system must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Rationale:

Preventing non-privileged users from executing privileged functions mitigates the risk that unauthorized individuals or processes may gain unnecessary access to information or privileges.

Privileged functions include, for example, establishing accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged 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 non-privileged users.

Audit:

If an HBSS or HIPS is active on the system, this is Not Applicable.

Verify the operating system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Get a list of authorized users (other than System Administrator and guest accounts) for the system.

Check the list against the system by using the following command:

```
# semanage login -l | more

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 must be mapped to the `sysadm_u` or `staff_u` users role.

All authorized non-administrative users must be mapped to the `user_u` role.

If they are not mapped in this way, refer to the remediation procedure below.

Remediation:

Configure the operating system to prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Utilizing the list of users gathered in the Audit section run the applicable command for that user below.

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>
```

References:

1. CCI: CCI-002165: The information system enforces organization-defined discretionary access control policies over defined subjects and objects.
2. NIST SP 800-53 Revision 4 :: AC-3 (4)
3. CCI-002235: The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.
4. NIST SP 800-53 Revision 4 :: AC-6 (10)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204444
Rule ID: SV-204444r754744_rule
STIG ID: RHEL-07-020020
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 <u>Define and Maintain Role-Based Access Control</u> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	4 <u>Controlled Use of Administrative Privileges</u> Controlled Use of Administrative Privileges			

1.6.1.10 Ensure system device files are labeled. (Manual)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that all system device files are correctly labeled to prevent unauthorized modification.

Rationale:

If an unauthorized or modified device is allowed to exist on the system, there is the possibility the system may perform unintended or unauthorized operations.

Audit:

Verify that all system device files are correctly labeled to prevent unauthorized modification.

List all device files on the system that are incorrectly labeled with the following commands:

Note: Device files are normally found under `/dev`, but applications may place device files in other directories and may necessitate a search of the entire system.

```
#find /dev -context *:device_t:* \( -type c -o -type b \) -printf "%p %Z\n"
#find /dev -context *:unlabeled_t:* \( -type c -o -type b \) -printf "%p
%Z\n"
```

Note: There are device files, such as `/dev/vmci`, that are used when the operating system is a host virtual machine. They will not be owned by a user on the system and require the `device_t` label to operate. These device files are not a finding.

If there is output from either of these commands, other than already noted, refer to the remediation procedure below.

Remediation:

Run the following command to determine which package owns the device file:

```
# rpm -qf <filename>
```

The package can be reinstalled from a `yum` repository using the command:

```
# sudo yum reinstall <packagename>
```

Alternatively, the package can be reinstalled from trusted media using the command:

```
# sudo rpm -Uvh <packagename>
```

References:

1. CCI-000318: The organization audits and reviews activities associated with configuration controlled changes to the system.
2. NIST SP 800-53 :: CM-3 e
3. NIST SP 800-53A :: CM-3.1 (v)
4. NIST SP 800-53 Revision 4 :: CM-3 f
5. CCI-000368: The organization documents any deviations from the established configuration settings for organization-defined information system components based on organization-defined operational requirements.
6. NIST SP 800-53 :: CM-6 c
7. NIST SP 800-53A :: CM-6.1 (v)
8. NIST SP 800-53 Revision 4 :: CM-6 c
9. CCI-001812: The information system prohibits user installation of software without explicit privileged status.
10. NIST SP 800-53 Revision 4 :: CM-11 (2)
11. CCI-001813: The information system enforces access restrictions.
12. NIST SP 800-53 Revision 4 :: CM-5 (1)
13. CCI-001814: The Information system supports auditing of the enforcement actions.
14. NIST SP 800-53 Revision 4 :: CM-5 (1)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204479
Rule ID: SV-204479r603261_rule
STIG ID: RHEL-07-020900
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

1.7 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/>

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
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

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

```
# echo "Authorized uses only. All activity may be monitored and reported." > /etc/issue
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.7.3 Ensure the Standard Mandatory DoD Notice and Consent Banner are configured (Automated)

Profile Applicability:

- STIG

Description:

The Red Hat Enterprise Linux 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.

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
Run the following command to verify the operating system displays a banner at the command line logon screen:

```
# more /etc/issue
```

Output should include:

```
"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."
```

Remediation:

Edit /etc/issue and replace the text with:

"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."

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204395
Rule ID: SV-204395r603261_rule
STIG ID: RHEL-07-010050
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.7.4 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

```
# echo "Authorized uses only. All activity may be monitored and reported." > /etc/issue.net
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.7.5 Ensure permissions on /etc/motd are 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 ownership it could be modified by unauthorized users with incorrect or misleading information.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `644` :

```
# stat /etc/motd
Access: (0644/-rw-r--r--)  Uid: (   0/   root)   Gid: (   0/   root)
```

Remediation:

Run the following commands to set permissions on `/etc/motd` :

```
# chown root:root /etc/motd
# chmod u-x,go-wx /etc/motd
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>14.6 Protect Information through Access Control Lists</u> 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.			

1.7.6 Ensure permissions on /etc/issue are 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 ownership it could be modified by unauthorized users with incorrect or misleading information.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and Access is `644` :

```
# stat /etc/issue
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set permissions on `/etc/issue` :

```
# chown root:root /etc/issue
# chmod u-x,go-wx /etc/issue
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

1.7.7 Ensure permissions on /etc/issue.net are 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 ownership it could be modified by unauthorized users with incorrect or misleading information.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and Access is `644` :

```
# stat /etc/issue.net
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set permissions on `/etc/issue.net` :

```
# chown root:root /etc/issue.net
# chmod u-x,go-wx /etc/issue.net
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

1.7.8 Ensure the Standard Mandatory DoD Notice and Consent Banner are configured (Manual)

Profile Applicability:

- STIG

Description:

The operating system must display the Standard Mandatory DoD Notice and Consent Banner immediately prior to, or as part of, remote access logon prompts.

Rationale:

Display of a standardized and approved use notification before granting access to the publicly accessible 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."

Audit:

Verify any publicly accessible connection to the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the system.

Check for the location of the banner file being used with the following command:

```
# grep -i banner /etc/ssh/sshd_config  
banner /etc/issue
```

This command will return the banner keyword and the name of the file that contains the ssh banner (in this case `/etc/issue`).

If the line is commented out, refer to the remediation procedure below.

View the file specified by the banner keyword to check that it matches the text of the Standard Mandatory DoD Notice and Consent 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."
```

If the system does not display a graphical logon banner or the banner does not match the Standard Mandatory DoD Notice and Consent Banner, refer to the remediation procedure below.

If the text in the file does not match the Standard Mandatory DoD Notice and Consent Banner, refer to the remediation procedure below.

Remediation:

Configure the operating system to display the Standard Mandatory DoD Notice and Consent Banner before granting access to the system via the ssh.

Edit the `/etc/ssh/sshd_config` file to uncomment the banner keyword and configure it to point to a file that will contain the logon banner (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).

Example: `vim /etc/sshd_config`

An example configuration line is:

```
banner /etc/issue
```

Either create the file containing the banner or replace the text in the file with the Standard Mandatory DoD Notice and Consent Banner.

Example: `vim /etc/issue`

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."
```

The SSH service must be restarted for changes to take effect.

Examples:

```
Type the following command:  
# /etc/init.d/sshd restart  
  
or use the service command:  
# service sshd restart  
  
or with systemd enter:  
$ sudo systemctl restart sshd
```

References:

1. CCI-000048: The information system displays an organization-defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance
2. NIST SP 800-53 :: AC-8 a
3. NIST SP 800-53A :: AC-8.1 (ii)
4. NIST SP 800-53 Revision 4 :: AC-8 a
5. CCI-000050: The information system retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access
6. NIST SP 800-53 :: AC-8 b
7. NIST SP 800-53A :: AC-8.1 (iii)
8. NIST SP 800-53 Revision 4 :: AC-8 b
9. CCI-001384: The information system, for publicly accessible systems, displays system use information organization-defined conditions before granting further access
10. NIST SP 800-53 :: AC-8 c
11. NIST SP 800-53A :: AC-8.2 (i)
12. NIST SP 800-53 Revision 4 :: AC-8 c 1
13. CCI-001385: The information system, for publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities
14. NIST SP 800-53 :: AC-8 c
15. NIST SP 800-53A :: AC-8.2 (ii)
16. NIST SP 800-53 Revision 4 :: AC-8 c 2
17. CCI-001386: The information system for publicly accessible systems displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities
18. NIST SP 800-53 :: AC-8 c
19. NIST SP 800-53A :: AC-8.2 (ii)
20. NIST SP 800-53 Revision 4 :: AC-8 c 2
21. CCI-001387: The information system for publicly accessible systems displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities
22. NIST SP 800-53 :: AC-8 c
23. NIST SP 800-53A :: AC-8.2 (ii)

- 24. NIST SP 800-53 Revision 4 :: AC-8 c 2
- 25. CCI-001388: The information system, for publicly accessible systems, includes a description of the authorized uses of the system
- 26. NIST SP 800-53 :: AC-8 c
- 27. NIST SP 800-53A :: AC-8.2 (iii)
- 28. NIST SP 800-53 Revision 4 :: AC-8 c 3

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204580
Rule ID: SV-204580r603261_rule
STIG ID: RHEL-07-040170
Severity: CAT II

1.8 GNOME Display Manager

The GNOME Display Manager (GDM) is a program that manages graphical display servers and handles graphical user logins.

The system will need to be re-booted, or brought down to run level 3 and back to run level 5 for changes to the GDM configuration to take effect.

Note: If GDM is not installed on the system, this section can be skipped

1.8.1 Ensure GDM login banner is configured (Manual)

Profile Applicability:

- 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.

Note: If a graphical login is not required, it should be removed to reduce the attack surface of the system.

Audit:

Verify that a file exists in `/etc/dconf/db/local.d/`: *(This is typically `/etc/dconf/db/local.d/01-banner-message`)*

Run the following command:

```
find /etc/dconf/db/local.d/ -type f -exec grep 'banner-message-' {} \;
```

Ensure the output includes:

```
banner-message-enable=true  
banner-message-text='<banner message>'
```

Remediation:

Edit or create the file `/etc/dconf/profile/local` and add the following:

```
user-db:user
system-db:local
file-db:/usr/share/local/greeter-dconf-defaults
```

Edit or create the file `/etc/dconf/db/local.d/` and add the following: *(This is typically `/etc/dconf/db/local.d/01-banner-message`)*

```
[org/gnome/login-screen]
banner-message-enable=true
banner-message-text='<banner message>'
```

Example Banner Text: 'Authorized users only. All activity may be monitored and reported.'
Run the following command to update the system databases:

```
# dconf update
```

Additional Information:

Additional options and sections may appear in the `/etc/dconf/db/local.d/01-banner-message` file.

If a different GUI login service is in use and required on the system, consult your documentation to disable displaying the last logged on user and apply an equivalent banner.

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204393
Rule ID: SV-204393r603261_rule
STIG ID: RHEL-07-010030
Severity: CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.8.2 Ensure Standard Mandatory DoD Notice and Consent Banner displayed via a graphical user logon (Manual)

Profile Applicability:

- STIG

Description:

The operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local access to the system via a graphical user logon.

Rationale:

Display of a standardized and approved use notification before granting access to the Ubuntu 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."
```

Audit:

Verify the Ubuntu operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a graphical user login.

Note: If the system does not have a graphical user interface installed, this requirement is Not Applicable.

Verify the operating system displays the exact approved Standard Mandatory DoD Notice and Consent Banner text with the command:

```
# grep banner-message-text /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.\nBy using this IS (which includes any
device attached to this IS), you consent to the following conditions:\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-At any time, the USG may
inspect and seize data stored on this IS.\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-This IS includes security measures (e.g., authentication and
access controls) to protect USG interests--not for your personal benefit or
privacy.\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. They will not be displayed on the Graphical User Interface.

If the banner-message-text is missing, commented out, or does not match the Standard Mandatory DoD Notice and Consent Banner exactly, this is a finding.

Remediation:

Configure the operating system to display the approved Standard Mandatory DoD Notice and Consent Banner before granting access to the system.

Note: If the system does not have a Graphical User Interface installed, this requirement is Not Applicable.

Create a database to contain the system-wide graphical user logon settings (if it does not already exist) with the following command:

```
# touch /etc/dconf/db/local.d/01-banner-message
```

Add the following line to the [org/gnome/login-screen] section of the "/etc/dconf/db/local.d/01-banner-message":

```
[org/gnome/login-screen]

banner-message-enable=true

banner-message-text='You are accessing a U.S. Government (USG) Information
System (IS) that is provided for USG-authorized use only.\nBy using this IS
(which includes any device attached to this IS), you consent to the following
conditions:\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-At any
time, the USG may inspect and seize data stored on this IS.\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-This IS includes security measures (e.g.,
authentication and access controls) to protect USG interests--not for your
personal benefit or privacy.\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. They will not be displayed on the Graphical User Interface.

Run the following command to update the database:

```
# dconf update
```

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204394
Rule ID: SV-204394r603261_rule
STIG ID: RHEL-07-010040
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.8.3 Ensure GDM session lock is enabled (Automated)

Profile Applicability:

- STIG

Description:

The Red Hat Enterprise Linux operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures.

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 re-authenticates. No other activity aside from re-authentication must unlock the system.

Audit:

Run the following command to verify `lock-enabled=true`

```
# grep -i 'lock-enabled' /etc/dconf/db/*.d/*  
lock-enabled=true
```

Remediation:

Edit or create the file `/etc/dconf/profile/gdm` and add the following:

```
user-db:user
system-db:gdm
file-db:/usr/share/gdm/greeter-dconf-defaults
```

Edit or create a file in `/etc/dconf/db/gdm.d/` and add the following: `_(This is typically /etc/dconf/db/gdm.d/00-screensaver)`

```
[org/gnome/desktop/screensaver]
# Set this to true to lock the screen when the screensaver activates
lock-enabled=true
```

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.

Additional Information:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204396
Rule ID: SV-204396r603261_rule
STIG ID: RHEL-07-010060
Severity: CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> 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	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

1.8.4 Ensure the graphical user Ctrl-Alt-Delete key sequence is disabled (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that the x86 Ctrl-Alt-Delete key sequence is disabled in the Graphical User Interface.

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 the graphical 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:

Note: If the operating system does not have a graphical user interface installed, this requirement is Not Applicable.

Verify the operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed.

Check that the ctrl-alt-del.target is masked and not active in the graphical user interface with the following command:

```
# grep logout /etc/dconf/db/local.d/*  
logout=''
```

If "logout" is not set to use two single quotations, or is missing, this is a finding.

Remediation:

Configure the system to disable the Ctrl-Alt-Delete sequence for the graphical user interface with the following command:

```
# touch /etc/dconf/db/local.d/00-disable-CAD
```

Add the setting to disable the Ctrl-Alt-Delete sequence for the graphical user interface:

```
[org/gnome/settings-daemon/plugins/media-keys]  
logout=''
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204456
Rule ID: SV-204456r603261_rule
STIG ID: RHEL-07-020231
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

1.8.5 Ensure users must authenticate users using MFA via a graphical user logon (Automated)

Profile Applicability:

- STIG

Description:

The operating system must uniquely identify and must authenticate users using multifactor authentication via a graphical user logon.

Rationale:

To assure accountability and prevent unauthenticated access, users must be identified and authenticated to prevent potential misuse and compromise of the system.

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 Common Access Card.

Satisfies: SRG-OS-000375-GPOS-00161,SRG-OS-000375-GPOS-00162

Audit:

Verify the operating system uniquely identifies and authenticates users using multifactor authentication via a graphical user logon.

Note: If the system does not have GNOME 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
```

Note: The example 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 enable-smartcard-authentication /etc/dconf/db/local.d/*
enable-smartcard-authentication=true
```

If "enable-smartcard-authentication" is set to "false" or the keyword is missing, this is a finding.

Remediation:

Configure the operating system to uniquely identify and authenticate users using multifactor authentication via a graphical user logon.

Note: If the system does not have GNOME installed, this requirement is Not Applicable.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

Note: The example 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-defaults
```

Edit `"[org/gnome/login-screen]"` and add or update the following line:

```
enable-smartcard-authentication=true
```

Update the system databases:

```
# dconf update
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.5 <u>Require MFA for Administrative Access</u> 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> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

1.8.6 Ensure GNOME Screensaver period of inactivity is configured (Automated)

Profile Applicability:

- STIG

Description:

The operating system must initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces.

Rationale:

A session time-out lock with the screensaver 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 screensaver is implemented at the point where session activity can be determined and/or controlled.

Impact:

Users must log out and back in again before the system-wide settings take effect.

Audit:

Verify the operating system initiates a screensaver after a 15-minute period of inactivity for graphical user interfaces.

The screen program must be installed to lock sessions on the console.

Note: If the system does not have GNOME installed, this requirement is Not Applicable.

Check to see if GNOME is configured to display a screensaver after a 15 minute delay with the following command:

```
# grep -i idle-delay /etc/dconf/db/local.d/*  
  
idle-delay=uint32 900
```

If the `idle-delay` setting is missing or is not set to 900 or less, refer to the remediation procedure below.

Remediation:

Configure the operating system to initiate a screensaver after a 15-minute period of inactivity for graphical user interfaces.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

```
# touch /etc/dconf/db/local.d/00-screensaver
```

Edit `/etc/dconf/db/local.d/00-screensaver` and add or update the following lines:

Set the lock time out to 900 seconds before the session is considered idle

You must include the `uint32` along with the integer key values as shown.

```
[org/gnome/desktop/session]
idle-delay=uint32 900
```

Update the system databases:

```
# dconf update
```

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204398
Rule ID: SV-204398r603261_rule
STIG ID: RHEL-07-010070
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> 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	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

1.8.7 Ensure screensaver lock-enabled is set (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 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.

The ability to enable/disable a session lock is given to the user by default. Disabling the user's ability to disengage the graphical user interface session lock provides the assurance that all sessions will lock after the specified period of time.

Audit:

Verify the operating system prevents a user from overriding the screensaver lock-enabled setting for the graphical user interface.

Note: If the system does not have GNOME installed, this requirement is Not Applicable. The screen program must be installed to lock sessions on the console.

Determine which profile the system database is using with the following command:

```
# grep system-db /etc/dconf/profile/user  
system-db:local
```

Check for the lock-enabled setting 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 a result, refer to the remediation procedure below.

Remediation:

Configure the operating system to prevent a user from overriding a screensaver lock after a 15-minute period of inactivity 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 setting to lock the screensaver lock-enabled setting:

```
/org/gnome/desktop/screensaver/lock-enabled
```

References:

1. CCI-000057: The information system initiates a session lock after the organization-defined time period of inactivity
2. NIST SP 800-53 :: AC-11 a
3. NIST SP 800-53A :: AC-11.1 (ii)
4. NIST SP 800-53 Revision 4 :: AC-11 a

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-214937
Rule ID: SV-214937r603261_rule
STIG ID: RHEL-07-010062
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> 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	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

1.8.8 Ensure overriding the screensaver lock-delay setting is prevented (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent a user from overriding the screensaver lock-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.

Audit:

Verify the operating system prevents a user from overriding a screensaver lock after a 15-minute period of inactivity for graphical user interfaces.

Note: If the system does not have GNOME installed, this requirement is Not Applicable. The screen program must be installed to lock sessions on the console.

Determine which profile the system database is using with the following command:

```
# grep system-db /etc/dconf/profile/user  
  
system-db:local
```

Check for the lock delay setting 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-delay /etc/dconf/db/local.d/locks/*  
  
/org/gnome/desktop/screensaver/lock-delay
```

If the command does not return a result, refer to the remediation procedure below.

Remediation:

Configure the operating system to prevent a user from overriding a screensaver lock after a 15-minute period of inactivity 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 setting to lock the screensaver lock delay:

```
/org/gnome/desktop/screensaver/lock-delay
```

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204399
Rule ID: SV-204399r603261_rule
STIG ID: RHEL-07-010081
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> 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	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

1.8.9 Ensure session idle-delay settings is enforced (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.

Audit:

Verify the operating system prevents a user from overriding session idle delay after a 15-minute period of inactivity for graphical user interfaces.

Note: If the system does not have GNOME installed, this requirement is Not Applicable. The screen program must be installed to lock sessions on the console.

Determine which profile the system database is using with the following command:

```
# grep system-db /etc/dconf/profile/user  
system-db:local
```

Check for the session idle delay setting 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-delay /etc/dconf/db/local.d/locks/  
/org/gnome/desktop/session/idle-delay
```

If the command does not return a result, refer to the remediation procedure below.

Remediation:

Configure the operating system to prevent a user from overriding a session lock after a 15-minute period of inactivity 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 setting to lock the session idle delay:

```
/org/gnome/desktop/session/idle-delay
```

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204400
Rule ID: SV-204400r603261_rule
STIG ID: RHEL-07-010082
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> 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	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

1.8.10 Ensure GNOME Idle activation is set (Automated)

Profile Applicability:

- STIG

Description:

The operating system must initiate a session lock for the screensaver after a period of inactivity for graphical user interfaces. As part of this configuration idle activation has to be configured.

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.

Impact:

Users must log out and back in again before the system-wide settings take effect.

Audit:

Verify the idle activation setting is configured correctly for GNOME so that when the operating system initiates a session lock after a 15-minute period of inactivity the screensaver is invoked. The screen program must be installed to lock sessions on the console.

If it is installed, GNOME must be configured to enforce a session lock after a 15-minute delay. Check for the session lock settings with the following commands:

```
# grep -i idle-activation-enabled /etc/dconf/db/local.d/*  
idle-activation-enabled=true
```

If `idle-activation-enabled` is not set to `true`, refer to the remediation procedure below.

Remediation:

Configure the operating system to initiate a session lock after a 15-minute period of inactivity for graphical user interfaces.

Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:

```
# touch /etc/dconf/db/local.d/00-screensaver
```

Add the setting to enable screensaver locking after 15 minutes of inactivity:

```
[org/gnome/desktop/screensaver]
idle-activation-enabled=true
```

Update the system databases:

```
# dconf update
```

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204402
Rule ID: SV-204402r603261_rule
STIG ID: RHEL-07-010100
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> 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	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

1.8.11 Ensure the screensaver idle-activation-enabled setting (Automated)

Profile Applicability:

- STIG

Description:

The operating system must prevent a user from overriding the screensaver idle-activation-enabled setting for the graphical user interface.

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.

The ability to enable/disable a session lock is given to the user by default. Disabling the user's ability to disengage the graphical user interface session lock provides the assurance that all sessions will lock after the specified period of time.

Audit:

Verify the operating system prevents a user from overriding the screensaver idle-activation-enabled setting for the graphical user interface.

Note: If the system does not have GNOME installed, this requirement is Not Applicable. The screen program must be installed to lock sessions on the console.

Determine which profile the system database is using with the following command:

```
# grep system-db /etc/dconf/profile/user  
  
system-db:local
```

Check for the idle-activation-enabled setting 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-activation-enabled /etc/dconf/db/local.d/locks/*  
  
/org/gnome/desktop/screensaver/idle-activation-enabled
```

If the command does not return a result, refer to the remediation procedure below.

Remediation:

Configure the operating system to prevent a user from overriding a screensaver lock after a 15-minute period of inactivity 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 setting to lock the screensaver idle-activation-enabled setting:

```
/org/gnome/desktop/screensaver/idle-activation-enabled
```


Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204403
Rule ID: SV-204403r603261_rule
STIG ID: RHEL-07-010101
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> 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	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

1.8.12 Ensure GNOME Lock Delay is configured (Automated)

Profile Applicability:

- STIG

Description:

The operating system must initiate a session lock for graphical user interfaces when the screensaver is activated. Please ensure the screensaver contains the lock delay system wide setting.

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.

Impact:

Users must log out and back in again before the system-wide settings take effect.

Audit:

Verify the lock delay setting is included in the system wide screensaver setting for the operating system.

Note: If the system does not have GNOME installed, this requirement is Not Applicable. The screen program must be installed to lock sessions on the console.

If GNOME is installed, check to see a session lock occurs when the screensaver is activated with the following command:

```
# grep -i lock-delay /etc/dconf/db/local.d/*  
lock-delay=uint32 5
```

If the `lock-delay` setting is missing, or is not set to 5 or less, and `uint32` is not included along with the integer key values as shown. Refer to the remediation procedure below.

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:

```
# touch /etc/dconf/db/local.d/00-screensaver
```

Add the setting to enable session locking when a screensaver is activated:

The `uint32` must be included along with the integer key values as shown.

```
[org/gnome/desktop/screensaver]
lock-delay=uint32 5
```

Update the system databases:

```
# dconf update
```

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204404
Rule ID: SV-204404r603261_rule
STIG ID: RHEL-07-010110
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> 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	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

1.8.13 Ensure automatic logon via GUI is not allowed (Automated)

Profile Applicability:

- STIG

Description:

The operating system must not allow an unattended or automatic logon to the system via a graphical user interface.

Rationale:

Failure to restrict system unattended or automatic logon to the system 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: If the system does not have GNOME 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`, refer to the remediation procedure below.

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`:

Example: `vim /etc/gdm/custom.conf`

```
[daemon]
AutomaticLoginEnable=false
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204432
Rule ID: SV-204432r603261_rule
STIG ID: RHEL-07-010440
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> 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	4.4 <u>Use Unique Passwords</u> 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.			

1.8.14 Ensure unrestricted logon is not allowed (Automated)

Profile Applicability:

- STIG

Description:

The operating system must not allow an unrestricted logon to the system.

Rationale:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Audit:

Verify the operating system does not allow an unrestricted logon to the system via a graphical user interface.

Note: If the system does not have GNOME installed, this requirement is Not Applicable.

Check for the value of the `TimedLoginEnable` parameter in `/etc/gdm/custom.conf` file with the following command:

```
# grep -i timedloginenable /etc/gdm/custom.conf  
TimedLoginEnable=false
```

If the value of `TimedLoginEnable` is not set to `false`, refer to the remediation procedure below.

Remediation:

Configure the operating system to not allow an unrestricted account to log on to the system via a graphical user interface.

Add or edit the line for the `TimedLoginEnable` parameter in the `[daemon]` section of the `/etc/gdm/custom.conf` file to `false`:

Example: `vim /etc/gdm/custom.conf`

```
[daemon]  
TimedLoginEnable=false
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204433
Rule ID: SV-204433r603261_rule
STIG ID: RHEL-07-010450
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> 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	4.4 <u>Use Unique Passwords</u> 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 graphical user interface automounter is disabled (Automated)

Profile Applicability:

- STIG

Description:

The Linux operating system must disable the graphical user interface automounter unless required.

Rationale:

Automatically mounting file systems permits easy introduction of unknown devices, thereby facilitating malicious activity.

Satisfies: SRG-OS-000114-GPOS-00059, SRG-OS-000378-GPOS-00163, SRG-OS-000480-GPOS-00227

Audit:

Note: If the operating system does not have a graphical user interface installed, this requirement is Not Applicable.

Verify the operating system disables the ability to automount devices in a graphical user interface.

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.

Check to see if automounter service is disabled with the following commands:

```
# cat /etc/dconf/db/local.d/00-No-Automount

[org/gnome/desktop/media-handling]

automount=false

automount-open=false

autorun-never=true
```

If the output does not match the example above, this is a finding.

```
# cat /etc/dconf/db/local.d/locks/00-No-Automount

/org/gnome/desktop/media-handling/automount

/org/gnome/desktop/media-handling/automount-open

/org/gnome/desktop/media-handling/autorun-never
```

If the output does not match the example, this is a finding.

Remediation:

Configure the graphical user interface to disable the ability to automount devices.

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.

Create or edit the /etc/dconf/db/local.d/00-No-Automount file and add the following:

```
[org/gnome/desktop/media-handling]

automount=false

automount-open=false

autorun-never=true
```

Create or edit the /etc/dconf/db/local.d/locks/00-No-Automount file and add the following:

```
/org/gnome/desktop/media-handling/automount

/org/gnome/desktop/media-handling/automount-open

/org/gnome/desktop/media-handling/autorun-never
```

Run the following command to update the database:

```
# dconf update
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b
5. CCI-000778: The information system uniquely identifies an organization defined list of specific and/or types of devices before establishing a local, remote, or network connection
6. NIST SP 800-53 :: IA-3
7. NIST SP 800-53A :: IA-3.1 (ii)
8. NIST SP 800-53 Revision 4 :: IA-3
9. CCI-001958: The information system authenticates an organization defined list of specific and/or types of devices before establishing a local, remote, or network connection
10. NIST SP 800-53 Revision 4 :: IA-3

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-219059
Rule ID: SV-219059r603261_rule
STIG ID: RHEL-07-020111
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.3 <u>Disable Autorun and Autoplay for Removable Media</u> Disable autorun and autoplay auto-execute functionality for removable media.			
v7	8.5 <u>Configure Devices Not To Auto-run Content</u> Configure devices to not auto-run content from removable media.			

1.9 Ensure updates, patches, and additional security software are installed (Manual)

Profile Applicability:

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

Description:

Periodically patches are released for included software either due to security flaws or to include additional functionality.

Note: Site policy may mandate a testing period before install onto production systems for available updates.

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 to verify there are no updates or patches to install.

```
# yum check-update
```

Remediation:

Use your package manager to update all packages on the system according to site policy. The following command will install all available packages

```
# yum update
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204459
Rule ID: SV-204459r603261_rule
STIG ID: RHEL-07-020260
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.3 Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v8	<u>7.4 Perform Automated Application Patch Management</u> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<u>3.4 Deploy Automated Operating System Patch Management Tools</u> 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	<u>3.5 Deploy Automated Software Patch Management Tools</u> 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.			

1.10 Ensure required packages for multifactor authentication are installed (Automated)

Profile Applicability:

- STIG

Description:

The operating system must have the required packages for multifactor authentication installed.

Rationale:

Using an authentication device, such as a 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 Common Access Card.

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.

Check for the presence of the packages required to support multifactor authentication with the following commands:

```
# yum list installed esc
esc-1.1.0-26.el7.noarch.rpm
# yum list installed pam_pkcs11
pam_pkcs11-0.6.2-14.el7.noarch.rpm
```

If the `esc` and `pam_pkcs11` packages are not installed, refer to the remediation procedure below.

Remediation:

To configure the operating system to implement multifactor authentication by installing the required packages.

Install the `esc` and `pam_pkcs11` packages on the system with the following command:

```
# yum install esc pam_pkcs11
```

References:

1. CCI-001948: The information system implements multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access
2. NIST SP 800-53 Revision 4 :: IA-2 (11)
3. CCI-001953: The information system accepts Personal Identity Verification (PIV) credentials
4. NIST SP 800-53 Revision 4 :: IA-2 (12)
5. CCI-001954: The information system electronically verifies Personal Identity Verification (PIV) credentials
6. NIST SP 800-53 Revision 4 :: IA-2 (12)

Additional Information:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204631
Rule ID: SV-204631r603261_rule
STIG ID: RHEL-07-041001
Severity: CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>6.5 Require MFA for Administrative Access</u> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.			
v7	<u>16.3 Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

1.11 Ensure anti-virus is installed and running (Manual)

Profile Applicability:

- STIG

Description:

The operating system must have virus scanning software installed.

Rationale:

Virus scanning software can be used to protect a system from penetration from computer viruses and to limit their spread through intermediate systems.

The virus scanning software should be configured to perform scans dynamically on accessed files. If this capability is not available, the system must be configured to scan, at a minimum, all altered files on the system on a daily basis.

If the system processes inbound SMTP mail, the virus scanner must be configured to scan all received mail.

Audit:

Verify an anti-virus solution is installed on the system. The anti-virus solution may be bundled with an approved host-based security solution.

If virus scanning software is not installed, refer to the remediation procedure below.

Remediation:

Install an antivirus solution on the system.

Document which solution is installed on the system with the ISSO.

References:

1. CCI-001668: The organization employs malicious code protection mechanisms at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means or inserted through the exploitation of information system vulnerabilities
2. NIST SP 800-53 :: SI-3 a
3. NIST SP 800-53A :: SI-3.1 (ii)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-214801
Rule ID: SV-214801r603261_rule
STIG ID: RHEL-07-032000
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 <u>Deploy and Maintain Anti-Malware Software</u> Deploy and maintain anti-malware software on all enterprise assets.			
v7	8.1 <u>Utilize Centrally Managed Anti-malware Software</u> Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.			

1.12 Ensure host-based intrusion detection tool is used (Manual)

Profile Applicability:

- STIG

Description:

The operating system must have a host-based intrusion detection tool installed.

Rationale:

Adding host-based intrusion detection 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:

Ask if a host-based intrusion detection application is loaded on the system. Per OPORD 16-0080, the preferred intrusion detection system is McAfee HBSS available through the U.S. Cyber Command (USCYBERCOM).

If another host-based intrusion detection application is in use, such as SELinux, this must be documented and approved.

Procedure:

Examine the system to determine if the Host Intrusion Prevention System (HIPS) is installed:

```
# rpm -qa | grep MFEhipdsm
```

Verify that the McAfee HIPS module is active on the system:

```
# ps -ef | grep -i "hipclient"
```

If the MFEhipdsm package is not installed, check for another intrusion detection system:

```
# find / -name <daemon name>
```

Where <daemon name> is the name of the primary application daemon to determine if the application is loaded on the system.

Determine if the application is active on the system:

```
# ps -ef | grep -i <daemon name>
```

If the `MFEhip1sm` package is not installed and an alternate host-based intrusion detection application has not been documented for use, refer to the remediation procedure below. If no host-based intrusion detection system is installed and running on the system, refer to the remediation procedure below.

Remediation:

Install and enable the latest `McAfee HIPS` package, available from USCYBERCOM.

Note: If the system does not support the McAfee HIPS package, install and enable a supported intrusion detection system application and document its use with the Authorizing Official.

References:

1. CCI-001263: The information system provides near real-time alerts when any of the organization defined list of compromise or potential compromise indicators occurs
2. NIST SP 800-53 :: SI-4 (5)
3. NIST SP 800-53A :: SI-4 (5).1 (ii)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-214800
Rule ID: SV-214800r754751_rule
STIG ID: RHEL-07-020019
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 <u>Deploy and Maintain Anti-Malware Software</u> Deploy and maintain anti-malware software on all enterprise assets.			
v7	8.1 <u>Utilize Centrally Managed Anti-malware Software</u> Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.			

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 inetd Services

inetd is a super-server daemon that provides internet services and passes connections to configured services. While not commonly used inetd and any unneeded inetd based services should be disabled if possible.

2.1.1 Ensure xinetd is not installed (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 are of the system.

Note: If an `xinetd` service or services are required, ensure that any `xinetd` service not required is stopped and disabled

Audit:

Run the following command to verify `xinetd` is not installed:

```
# rpm -q xinetd  
package xinetd is not installed
```

Remediation:

Run the following command to remove `xinetd`:

```
# yum remove xinetd
```

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> 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>2.6 Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2 Special Purpose 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, or the service be masked to reduce the potential attack surface.

2.2.1 Time Synchronization

It is recommended that physical systems and virtual guests lacking direct access to the physical host's clock be configured to synchronize their time using a service such as NTP or chrony.

2.2.1.1 Ensure time synchronization is in use (Manual)

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.
- Only **one** time synchronization package should be installed

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 a time synchronization packages is installed:

```
# rpm -q chrony ntp
chrony-<version>
# rpm -q ntp
ntp-<version>
```

Remediation:

Run **One** of the following commands to install chrony **or** NTP:

To install chrony, run the following command:

```
# yum install chrony
```

OR

To install ntp, run the following command:

```
# yum install ntp
```

Note: On systems where host based time synchronization is available consult your virtualization software documentation and setup host based synchronization.

Additional Information:

- On systems where host based time synchronization is not available, verify that chrony *or* NTP 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	8.4 <u>Standardize Time Synchronization</u> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.			
v7	6.1 <u>Utilize Three Synchronized Time Sources</u> 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.			

2.2.1.2 Ensure chrony is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`chrony` is a daemon which implements the Network Time Protocol (NTP) and is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. More information on `chrony` can be found at <http://chrony.tuxfamily.org/>. `chrony` can be configured to be a client and/or a server.

Rationale:

If `chrony` is in use on the system proper configuration is vital to ensuring time synchronization is working properly.

Note: This recommendation only applies if `chrony` is in use on the system.

Audit:

IF `chrony` is installed on the system:

Run the following command and verify remote server is configured properly:

```
# grep -E "^(server|pool)" /etc/chrony.conf
server <remote-server>
```

Multiple servers may be configured.

Run the following command and verify `OPTIONS` includes `'-u chrony'`:

```
# grep ^OPTIONS /etc/sysconfig/chronyd
OPTIONS="-u chrony"
```

Additional options may be present.

Remediation:

Add or edit server or pool lines to `/etc/chrony.conf` as appropriate:

```
server <remote-server>
```

Add or edit the `OPTIONS` in `/etc/sysconfig/chronyd` to include `'-u chrony'`:

```
OPTIONS="-u chrony"
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 <u>Standardize Time Synchronization</u> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.			
v7	6.1 <u>Utilize Three Synchronized Time Sources</u> 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.			

2.2.1.3 Ensure ntp is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

ntp is a daemon which implements the Network Time Protocol (NTP). It is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. More information on NTP can be found at <http://www.ntp.org>. ntp can be configured to be a client and/or a server.

Note: This recommendation only applies if ntp is in use on the system.

Rationale:

If ntp is in use on the system proper configuration is vital to ensuring time synchronization is working properly.

Audit:

IF NTP is installed on the system:

Run the following command and verify ntpd is enabled:

```
# systemctl is-enabled ntpd  
  
enabled
```

Run the following command and verify output matches:

```
# grep "^restrict" /etc/ntp.conf  
  
restrict -4 default kod nomodify notrap nopeer noquery  
restrict -6 default kod nomodify notrap nopeer noquery
```

The -4 in the first line is optional and options after default can appear in any order.

Additional restriction lines may exist.

Run the following command and verify remote server is configured properly:

```
# grep -E "^(server|pool)" /etc/ntp.conf  
  
server <remote-server>
```

Multiple servers may be configured

Run the following commands and verify that '-u ntp:ntp' is included in `OPTIONS` OR `ExecStart` as listed:

```
# grep "^OPTIONS" /etc/sysconfig/ntpd  
  
OPTIONS="-u ntp:ntp"
```

OR

```
# grep "^ExecStart" /usr/lib/systemd/system/ntpd.service  
  
ExecStart=/usr/sbin/ntpd -u ntp:ntp $OPTIONS
```

Additional options may be present.

Remediation:

Add or edit restrict lines in `/etc/ntp.conf` to match the following:

```
restrict -4 default kod nomodify notrap nopeer noquery  
restrict -6 default kod nomodify notrap nopeer noquery
```

Add or edit server or pool lines to `/etc/ntp.conf` as appropriate:

```
server <remote-server>
```

Add or edit the `OPTIONS` in `/etc/sysconfig/ntpd` to include `'-u ntp:ntp'`:

```
OPTIONS="-u ntp:ntp"
```

Reload the systemd daemon:

```
systemctl daemon-reload
```

Enable and start the ntp service:

```
systemctl --now enable ntpd
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 <u>Standardize Time Synchronization</u> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.			
v7	6.1 <u>Utilize Three Synchronized Time Sources</u> 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.			

2.2.1.4 Ensure internal information system clocks are synchronizing (Automated)

Profile Applicability:

- STIG

Description:

The Linux operating system must, for networked systems, synchronize clocks with a server that is synchronized to one of the redundant United States Naval Observatory (USNO) time servers, 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).

Satisfies: SRG-OS-000355-GPOS-00143, SRG-OS-000356-GPOS-00144

Audit:

Check to see if NTP is running in continuous mode:

```
# ps -ef | grep ntp
```

If NTP is not running, check to see if "chronyd" is running in continuous mode:

```
# ps -ef | grep chronyd
```

If NTP or "chronyd" is not running, this is a finding.

If the NTP process is found, then check the "ntp.conf" file for the "maxpoll" option setting:

```
# grep maxpoll /etc/ntp.conf  
server 0.rhel.pool.ntp.org iburst maxpoll 10
```

If the option is set to "17" or is not set, this is a finding.

If the file does not exist, check the "/etc/cron.daily" subdirectory for a crontab file controlling the execution of the "ntpd -q" command.

```
# grep -i "ntpd -q" /etc/cron.daily/*  
# ls -al /etc/cron.* | grep ntp  
ntp
```

If a crontab file does not exist in the "/etc/cron.daily" that executes the "ntpd -q" command, this is a finding.

If the "chronyd" process is found, then check the "chrony.conf" file for the "maxpoll" option setting:

```
# grep maxpoll /etc/chrony.conf  
server 0.rhel.pool.ntp.org iburst maxpoll 10
```

If the option is not set or the line is commented out, this is a finding

Remediation:

Edit the `/etc/ntp.conf` or `/etc/chrony.conf` file and add or update an entry to define "maxpoll" to "10" as follows:

```
server 0.rhel.pool.ntp.org iburst maxpoll 10
```

If NTP was running and "maxpoll" was updated, the NTP service must be restarted:

```
# systemctl restart ntpd
```

If NTP was not running, it must be started:

```
# systemctl start ntpd
```

If "chronyd" was running and "maxpoll" was updated, the service must be restarted:

```
# systemctl restart chronyd.service
```

If "chronyd" was not running, it must be started:

```
# systemctl start chronyd.service
```

References:

1. CCI-001891: The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source
2. NIST SP 800-53 Revision 4 :: AU-8 (1) (a)
3. CCI-002046: The information system synchronizes the internal system clocks to the authoritative time source when the time difference is greater than the organization-defined time period
4. NIST SP 800-53 Revision 4 :: AU-8 (1) (b)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204603
Rule ID: SV-204603r603261_rule
STIG ID: RHEL-07-040500
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 <u>Standardize Time Synchronization</u> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.			
v7	6.1 <u>Utilize Three Synchronized Time Sources</u> 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.			

2.2.2 Ensure X11 Server components are not installed (Automated)

Profile Applicability:

- Level 1 - 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:

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:

Run the following command to Verify X Windows Server is not installed.

```
# rpm -qa xorg-x11-server*
```

Remediation:

Run the following command to remove the X Windows Server packages:

```
# yum remove xorg-x11-server*
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204624
Rule ID: SV-204624r646847_rule
STIG ID: RHEL-07-040730
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> 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>2.6 Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			

2.2.3 Ensure Avahi Server is not installed (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.

Audit:

Run one of the following command to verify `avahi-autoipd` and `avahi` are not installed:

```
# rpm -q avahi-autoipd avahi
package avahi-autoipd is not installed
package avahi is not installed
```

Remediation:

Run the following commands to stop, mask and remove `avahi-autoipd` and `avahi`:

```
# systemctl stop avahi-daemon.socket avahi-daemon.service
# yum remove avahi-autoipd avahi
```


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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.4 Ensure CUPS is not installed (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.

Note: Removing CUPS will prevent printing from the system

Impact:

Disabling CUPS will prevent printing from the system, a common task for workstation systems.

Audit:

Run the following command to verify `cups` is not installed:

```
# rpm -q cups
package cups is not installed
```

Remediation:

Run the following command to remove `cups`:

```
# yum remove cups
```

References:

1. More detailed documentation on CUPS is available at the project homepage at <http://www.cups.org>.

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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.5 Ensure DHCP Server is not installed (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.

Rationale:

Unless a system is specifically set up to act as a DHCP server, it is recommended that the dhcp package be removed to reduce the potential attack surface.

Audit:

Run the following command to verify dhcp is not installed:

```
# rpm -q dhcp  
package dhcp is not installed
```

Remediation:

Run the following command to remove dhcp:

```
# yum remove dhcp
```

References:

1. dhcpd(8)

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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.6 Ensure LDAP server is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - 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 server, it is recommended that the software be removed to reduce the potential attack surface.

Audit:

Run the following command to verify `openldap-servers` is not installed:

```
# rpm -q openldap-servers
package openldap-servers is not installed
```

Remediation:

Run the following command to remove `openldap-servers`:

```
# yum remove openldap-servers
```

References:

1. For more detailed documentation on OpenLDAP, go to the project homepage at <http://www.openldap.org>.

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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.7 Ensure DNS Server is not installed (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.

Audit:

Run one of the following commands to verify `bind` is not installed:

```
# rpm -q bind  
package bind is not installed
```

Remediation:

Run the following command to remove `bind`:

```
# yum remove bind
```


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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.8 Ensure FTP Server is not installed (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:

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.

Note: Additional FTP servers also exist and should be removed if not required.

Audit:

Run the following command to verify `vsftpd` is not installed:

```
# rpm -q vsftpd  
package vsftpd is not installed
```

Remediation:

Run the following command to remove `vsftpd`:

```
# yum remove vsftpd
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204620
Rule ID: SV-204620r603261_rule
STIG ID: RHEL-07-040690
Severity: CAT I

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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.9 Ensure HTTP server is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

HTTP or web servers provide the ability to host web site content.

Rationale:

Unless there is a need to run the system as a web server, it is recommended that the package be removed to reduce the potential attack surface.

Notes:

- *Several http servers exist. `apache`, `apache2`, `lighttpd`, and `nginx` are example packages that provide an HTTP server.*
- *These and other packages should also be audited, and removed if not required.*

Audit:

Run the following command to verify `httpd` is not installed:

```
# rpm -q httpd  
package httpd is not installed
```

Remediation:

Run the following command to remove `httpd`:

```
# yum remove httpd
```

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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.10 Ensure IMAP and POP3 server is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`dovecot` is an open source IMAP and POP3 server 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.

Notes:

- *Several IMAP/POP3 servers exist and can use other service names. `courier-imap` and `cyrus-imap` are example services that provide a mail server.*
- *These and other services should also be audited and the packages removed if not required.*

Audit:

Run the following command to verify `dovecot` is not installed:

```
# rpm -q dovecot  
package dovecot is not installed
```

Remediation:

Run the following command to remove `dovecot`:

```
# yum remove dovecot
```

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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.11 Ensure Samba is not installed (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.

Audit:

Run the following command to verify `samba` is not installed:

```
# rpm -q samba  
package samba is not installed
```

Remediation:

Run the following command to remove `samba`:

```
# yum remove samba
```


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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.12 Ensure HTTP Proxy Server is not installed (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.

Audit:

Run the following command to verify `squid` is not installed:

```
# rpm -q squid  
package squid is not installed
```

Remediation:

Run the following command to remove the `squid` package:

```
# yum remove squid
```

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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.13 Ensure net-snmp is not installed (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.*

Audit:

Run the following command to verify `net-snmp` is not installed:

```
# rpm -q net-snmp  
package net-snmp is not installed
```

Remediation:

Run the following command to remove `net-snmpd`:

```
# yum remove net-snmp
```

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> 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>2.6 Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.14 Ensure NIS server is not installed (Automated)

Profile Applicability:

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

Description:

The `ypserv` package provides the Network Information Service (NIS). This service, formally known as Yellow Pages, is a client-server directory service protocol for distributing system configuration files. The NIS server is a collection of programs that allow for the distribution of 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 `ypserv` package be removed, and if required a more secure services be used.

Audit:

Run the following command to verify `ypserv` is not installed:

```
# rpm -q ypserv  
package ypserv is not installed
```

Remediation:

Run the following command to remove `ypserv`:

```
# yum remove ypserv
```

References:

1. CCI: CCI-000381: The organization configures the information system to provide only essential capabilities.
2. NIST SP 800-53 :: CM-7
3. NIST SP 800-53A :: CM-7.1 (ii)
4. NIST SP 800-53 Revision 4 :: CM-7 a

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204443
Rule ID: SV-204443r603261_rule
STIG ID: RHEL-07-020010
Severity: CAT I

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> 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>2.6 Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.15 Ensure telnet-server is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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.

Audit:

Run the following command to verify the `telnet-server` package is not installed:

```
rpm -q telnet-server  
package telnet-server is not installed
```

Remediation:

Run the following command to remove the `telnet-server` package:

```
# yum remove telnet-server
```


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> 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>2.6 Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.16 Ensure mail transfer agent is 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.

Notes:

- *This recommendation 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.*

Audit:

Run the following command to verify that the MTA is not listening on any non-loopback address (127.0.0.1 or ::1)
Nothing should be returned

```
# ss -ltnu | grep -E ':25\s' | grep -E -v '\s(127.0.0.1|\\[?::1\\]):25\s'
```

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
```

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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.17 Ensure *nfs-utils* is not installed or the *nfs-server* service is masked (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 network shares, it is recommended that the *nfs-utils* package be removed to reduce the attack surface of the system.

Audit:

Run the following command to verify *nfs-utils* is not installed:

```
# rpm -q nfs-utils
package nfs-utils is not installed
```

OR

If the *nfs*-package is required as a dependency, run the following command to verify that the *nfs-server* service is masked:

```
# systemctl is-enabled nfs-server
masked
```

Remediation:

Run the following command to remove `nfs-utils`:

```
# yum remove nfs-utils
```

OR

If the `nfs`-package is required as a dependency, run the following command to stop and mask the `nfs-server` service:

```
# systemctl --now mask nfs-server
```

Additional Information:

many of the libvirt packages used by Enterprise Linux virtualization are dependent on the `nfs-utils` package. If the `nfs`-package is required as a dependency, the `nfs-server` 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	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.18 Ensure rpcbind is not installed or the rpcbind services are masked (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 that the rpcbind package be removed to reduce the attack surface of the system.

Audit:

Run the following command to verify `rpcbind` is not installed:

```
# rpm -q rpcbind  
package rpcbind is not installed
```

OR

If the `rpcbind` package is required as a dependency, run the following commands to verify that the `rpcbind` and `rpcbind.socket` services are masked:

```
# systemctl is-enabled rpcbind  
masked  
# systemctl is-enabled rpcbind.socket  
masked
```

Remediation:

Run the following command to remove `nfs-utils`:

```
# yum remove rpcbind
```

OR

If the `rpcbind` package is required as a dependency, run the following commands to stop and mask the `rpcbind` and `rpcbind.socket` services:

```
# systemctl --now mask rpcbind  
# systemctl --now mask rpcbind.socket
```

Additional Information:

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` is required as a dependency, the services `rpcbind.service` and `rpcbind.socket` should be stopped and masked to reduce the attack surface of the system.

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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.19 Ensure rsync is not installed or the rsyncd service is masked (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` package should be removed to reduce the attack surface area of the system.

The `rsyncd` service presents a security risk as it uses unencrypted protocols for communication.

Note: If a required dependency exists for the `rsync` package, but the `rsyncd` service is not required, the service should be masked.

Impact:

There are packages that are dependent on the `rsync` package. If the `rsync` package is removed, these packages will be removed as well.

Before removing the `rsync` package, review any dependent packages to determine if they are required on the system. If a dependent package is required, mask the `rsyncd` service and leave the `rsync` package installed.

Audit:

Run the following command to verify that `rsync` is not installed:

```
# rpm -q rsync  
package rsync is not installed
```

OR

Run the following command to verify the `rsyncd` service is masked:

```
# systemctl is-enabled rsyncd  
masked
```

Remediation:

Run the following command to remove the `rsync` package:

```
# yum remove rsync
```

OR

Run the following command to mask the `rsyncd` service:

```
# systemctl --now mask rsyncd
```

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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.20 Ensure the rsh package has been removed (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.

Audit:

Check to see if the `rsh-server` package is installed with the following command:

```
# yum list installed rsh-server
```

If the `rsh-server` package is installed, refer to the remediation procedure below.

Remediation:

Configure the operating system to disable non-essential capabilities by removing the `rsh-server` package from the system with the following command:

```
# yum remove rsh-server
```

References:

1. CCI: CCI-000381: The organization configures the information system to provide only essential capabilities.
2. NIST SP 800-53 :: CM-7
3. NIST SP 800-53A :: CM-7.1 (ii)
4. NIST SP 800-53 Revision 4 :: CM-7 a

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204442
Rule ID: SV-204442r603261_rule
STIG ID: RHEL-07-020000
Severity: CAT I

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> 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>2.6 Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			

2.2.21 Ensure the TFTP server has not been installed (Automated)

Profile Applicability:

- STIG

Description:

The operating system must not have the Trivial File Transfer Protocol (TFTP) server package 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.

Check to see if a TFTP server has been installed with the following command:

```
# yum list installed tftp-server  
tftp-server-0.49-9.el7.x86_64.rpm
```

If TFTP is installed and the requirement for TFTP is not documented with the Authorizing Official, refer to the remediation procedure below.

Remediation:

Remove the TFTP package from the system with the following command:

```
# yum remove tftp-server
```

References:

1. CCI-000318: The organization audits and reviews activities associated with configuration controlled changes to the system
2. NIST SP 800-53 :: CM-3 e
3. NIST SP 800-53A :: CM-3.1 (v)
4. NIST SP 800-53 Revision 4 :: CM-3 f
5. CCI-000368: The organization documents any deviations from the established configuration settings for organization-defined information system components based on organization-defined operational requirements
6. NIST SP 800-53 :: CM-6 c
7. NIST SP 800-53A :: CM-6.1 (v)
8. NIST SP 800-53 Revision 4 :: CM-6 c
9. CCI-001812: The information system prohibits user installation of software without explicit privileged status
10. NIST SP 800-53 Revision 4 :: CM-11 (2)
11. CCI-001813: The information system enforces access restrictions.
12. NIST SP 800-53 Revision 4 :: CM-5 (1)
13. CCI-001814: The Information system supports auditing of the enforcement actions.
14. NIST SP 800-53 Revision 4 :: CM-5 (1)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204621
Rule ID: SV-204621r603261_rule
STIG ID: RHEL-07-040700
Severity: CAT I

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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.22 Ensure TFTP daemon is configured to operate in secure mode (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that if the Trivial File Transfer Protocol (TFTP) server is required, the TFTP daemon is 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.

Check to see if a TFTP server has been installed with the following commands:

```
# yum list installed tftp-server  
  
tftp-server.x86_64 x.x-x.el7 rhel-7-server-rpms
```

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, refer to the remediation procedure below.

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):

Example: vim /etc/xinetd.d/tftp

Add this line.

```
server_args = -s /var/lib/tftpboot
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204623
Rule ID: SV-204623r603261_rule
STIG ID: RHEL-07-040720
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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.23 Ensure default SNMP community strings don't exist (Automated)

Profile Applicability:

- STIG

Description:

SNMP community strings must be changed from the default values.

Rationale:

Whether active or not, default Simple Network Management Protocol (SNMP) community strings must be changed to maintain security. If the service is running with the default authenticators, anyone can gather data about the system and the network and use the information to potentially compromise the integrity of the system or network(s). It is highly recommended that SNMP version 3 user authentication and message encryption be used in place of the version 2 community strings.

Audit:

Verify that a system using SNMP is not using default community strings.

Check to see if the `/etc/snmp/snmpd.conf` file exists with the following command:

```
# ls -al /etc/snmp/snmpd.conf
-rw----- 1 root root 52640 Mar 12 11:08 snmpd.conf
```

If the file does not exist, this is Not Applicable.

If the file does exist, check for the default community strings with the following commands:

```
# grep public /etc/snmp/snmpd.conf
# grep private /etc/snmp/snmpd.conf
```

If either of these commands returns any output, refer to the remediation procedure below.

Remediation:

If the `/etc/snmp/snmpd.conf` file exists, modify any lines that contain a community string value of `public` or `private` to another string value.

Example: `vim /etc/snmp/snmpd.conf`

Example of changing the `public` and `private` string value:

```
snmp-server community nEV8rM1ndthi$ RO
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204627
Rule ID: SV-204627r603261_rule
STIG ID: RHEL-07-040800
Severity: CAT I

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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.24 Ensure NFS is configured to use RPCSEC_GSS (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that the Network File System (NFS) is configured to use RPCSEC_GSS.

Rationale:

When an NFS server is configured to use RPCSEC_SYS, a selected userid and groupid are used to handle requests from the remote user. The userid and groupid could mistakenly or maliciously be set incorrectly. The RPCSEC_GSS method of authentication uses certificates on the server and client systems to more securely authenticate the remote mount request.

Audit:

Verify `AUTH_GSS` is being used to authenticate NFS mounts.

To check if the system is importing an NFS file system, look for any entries in the `/etc/fstab` file that have a file system type of `nfs` with the following command:

```
# cat /etc/fstab | grep nfs  
192.168.21.5:/mnt/export /data1 nfs4 rw, sync , soft, sec=krb5:krb5i:krb5p
```

If the system is mounting file systems via NFS and has the `sec` option without the `krb5:krb5i:krb5p` settings, the `sec` option has the `sys` setting, or the `sec` option is missing, refer to the remediation procedure below.

Remediation:

Update the `/etc/fstab` file so the option `sec` is defined for each NFS mounted file system and the `sec` option does not have the `sys` setting.

Example: `vim /etc/fstab`

Ensure the `sec` option is defined as `krb5:krb5i:krb5p`.

```
192.168.21.5:/mnt/export /data1 nfs4 rw, sync , soft, sec=krb5:krb5i:krb5p
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204626
Rule ID: SV-204626r603261_rule
STIG ID: RHEL-07-040750
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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.25 Ensure unrestricted mail relaying is prevented (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:

```
# yum list installed postfix
postfix-2.6.6-6.el7.x86_64.rpm
```

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`, refer to the remediation procedure below.

Remediation:

If `postfix` is installed, modify the `/etc/postfix/main.cf` file to restrict client connections to the local network with the following command:

Example: `vim /etc/postfix/main.cf`

Add this line:

```
# postconf -e 'smtpd_client_restrictions = permit_mynetworks,reject'
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204619
Rule ID: SV-204619r603261_rule
STIG ID: RHEL-07-040680
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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.26 Ensure `ldap_tls_cacert` is set for LDAP. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications is set for `ldap_tls_cacert`.

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

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 key used to generate the hash.

Audit:

If LDAP is not being utilized, this requirement is Not Applicable.

Verify the operating system implements cryptography to protect the integrity of remote LDAP access sessions.

To determine if LDAP is being used for authentication, use the following command:

```
# systemctl status sssd.service
sssd.service - System Security Services Daemon
Loaded: loaded (/usr/lib/systemd/system/sss.service; enabled; vendor preset: disabled)
Active: active (running) since Wed 2018-06-27 10:58:11 EST; 1h 50min ago
```

If the `sss.service` is active, then LDAP is being used.

Check that the path to the X.509 certificate for peer authentication with the following command:

```
# grep -i tls_cacert /etc/sss/sss.conf
ldap_tls_cacert = /etc/pki/tls/certs/ca-bundle.crt
```

Verify the `ldap_tls_cacert` option points to a file that contains the trusted CA certificate. If this file does not exist, or the option is commented out or missing, refer to the remediation procedure.

Remediation:

Configure the operating system to implement cryptography to protect the integrity of LDAP remote access sessions.

Add or modify the following line in `/etc/sss/sss.conf`:

Example: `vim /etc/sss/sss.conf`

Add, uncomment or update the following line:

```
ldap_tls_cacert = /etc/pki/tls/certs/ca-bundle.crt
```

References:

1. CCI-001453: The information system implements cryptographic mechanisms to protect the integrity of remote access sessions
2. NIST SP 800-53 :: AC-17 (2)
3. NIST SP 800-53A :: AC-17 (2).1
4. NIST SP 800-53 Revision 4 :: AC-17 (2)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204583
Rule ID: SV-204583r603261_rule
STIG ID: RHEL-07-040200
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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.27 Ensure `ldap_id_use_start_tls` is set for LDAP. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) authentication communications setting `ldap_id_use_start_tls`.

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

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 key used to generate the hash.

Audit:

NOTE *** If LDAP is not being utilized, this requirement is Not Applicable.

Verify the operating system implements cryptography to protect the integrity of remote LDAP authentication sessions.

To determine if LDAP is being used for authentication, use the following command:

```
# systemctl status sssd.service
sssd.service - System Security Services Daemon
Loaded: loaded (/usr/lib/systemd/system/sss.service; enabled; vendor preset: disabled)
Active: active (running) since Wed 2018-06-27 10:58:11 EST; 1h 50min ago
```

If the `sssd.service` is active, then LDAP is being used. To see if LDAP is configured to use TLS, use the following command:

```
# grep -i "start_tls" /etc/sss/sss.conf
ldap_id_use_start_tls = true
```

If the `ldap_id_use_start_tls` option is not `true`, refer to the remediation procedure below.

Remediation:

Configure the operating system to implement cryptography to protect the integrity of LDAP authentication sessions.

Add or modify the following line in `/etc/sss/sss.conf`:

Example: `vim /etc/sss/sss.conf`

Add, uncomment or update the following line:

```
ldap_id_use_start_tls = true
```

References:

1. CCI-001453: The information system implements cryptographic mechanisms to protect the integrity of remote access sessions
2. NIST SP 800-53 :: AC-17 (2)
3. NIST SP 800-53A :: AC-17 (2).1
4. NIST SP 800-53 Revision 4 :: AC-17 (2)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204581
Rule ID: SV-204581r603261_rule
STIG ID: RHEL-07-040180
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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.2.28 Ensure `ldap_tls_reqcert` is set for LDAP (Automated)

Profile Applicability:

- STIG

Description:

The operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications by setting `ldap_tls_reqcert`.

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

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 key used to generate the hash.

Audit:

NOTE*** If LDAP is not being utilized, this requirement is Not Applicable.

Verify the operating system implements cryptography to protect the integrity of remote LDAP access sessions.

To determine if LDAP is being used for authentication, use the following command:

```
# systemctl status sssd.service
sssd.service - System Security Services Daemon
Loaded: loaded (/usr/lib/systemd/system/sssd.service; enabled; vendor preset: disabled)
Active: active (running) since Wed 2018-06-27 10:58:11 EST; 1h 50min ago
```

If the `sssd.service` is active, then LDAP is being used.

Verify that the `sssd` service is configured to require the use of certificates:

```
# grep -i tls_reqcert /etc/sssd/sssd.conf

ldap_tls_reqcert = demand
```

If the `ldap_tls_reqcert` setting is missing, commented out, or does not exist, refer to the remediation procedure below.

If the `ldap_tls_reqcert` setting is not set to `demand` or `hard`, refer to the remediation procedure below.

Remediation:

Configure the operating system to implement cryptography to protect the integrity of LDAP remote access sessions.

Add or modify the following line in `/etc/sss/sss.conf`:

Example: `vim /etc/sss/sss.conf`

Add, uncomment or update the following line:

```
ldap_tls_reqcert = demand
```

References:

1. CCI-001453: The information system implements cryptographic mechanisms to protect the integrity of remote access sessions
2. NIST SP 800-53 :: AC-17 (2)
3. NIST SP 800-53A :: AC-17 (2).1
4. NIST SP 800-53 Revision 4 :: AC-17 (2)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204582
Rule ID: SV-204582r603261_rule
STIG ID: RHEL-07-040190
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software 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 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

2.3 Service Clients

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.

2.3.1 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:

```
# yum remove ypbind
```

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> 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>2.6 Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			

2.3.2 Ensure rsh client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `rsh` package contains the client commands for the `rsh` services.

Rationale:

These legacy clients contain numerous security exposures and have been replaced with the more secure SSH package. Even if the server is removed, it is best to ensure the clients are also removed to prevent users from inadvertently attempting to use these commands and therefore exposing their credentials. Note that removing the `rsh` package removes the clients for `rsh`, `rcp` and `rlogin`.

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 `rsh` package is not installed:

```
# rpm -q rsh  
package rsh is not installed
```

Remediation:

Run the following command to remove the `rsh` package:

```
# yum remove rsh
```


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> 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>2.6 Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			

2.3.3 Ensure talk client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `talk` software makes it possible for users to send and receive messages across systems through a terminal session. The `talk` client, which allows initialization of talk sessions, is installed by default.

Rationale:

The software presents a security risk as it uses unencrypted protocols for communication.

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 `talk` package is not installed:

```
# rpm -q talk  
package talk is not installed
```

Remediation:

Run the following command to remove the `talk` package:

```
# yum remove talk
```

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> 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>2.6 Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			

2.3.4 Ensure telnet client is not installed (Automated)

Profile Applicability:

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

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:

```
# yum remove telnet
```

References:

1. CCI: CCI-000381: The organization configures the information system to provide only essential capabilities.
2. NIST SP 800-53 :: CM-7
3. NIST SP 800-53A :: CM-7.1 (ii)
4. NIST SP 800-53 Revision 4 :: CM-7 a

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204502
Rule ID: SV-204502r603261_rule
STIG ID: RHEL-07-021710
Severity: CAT I

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> 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>2.6 Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			

2.3.5 Ensure LDAP client is not installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - 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:

```
# yum remove openldap-clients
```

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> 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>2.6 Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			

2.4 Ensure nonessential services are removed or masked (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.

Audit:

Run the following command:

```
# lsof -i -P -n | grep -v "(ESTABLISHED)"
```

Review the output to ensure that all services listed are required on the system. If a listed service is not required, remove the package containing the service. If the package containing the service is required, stop and mask the service

Remediation:

Run the following command to remove the package containing the service:

```
# yum remove <package_name>
```

OR If required packages have a dependency:

Run the following command to stop and mask the service:

```
# systemctl --now mask <service_name>
```

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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

3 Network Configuration

This section provides guidance on for securing the network configuration of the system through kernel parameters, access list control, and firewall settings.

3.1 Disable unused network protocols and devices

To reduce the attack surface of a system, unused network protocols and devices should be disabled.

3.1.1 Disable IPv6 (Manual)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Although IPv6 has many advantages over IPv4, not all organizations have IPv6 or dual stack configurations implemented.

Rationale:

If IPv6 or dual stack is not to be used, it is recommended that IPv6 be disabled to reduce the attack surface of the system.

Impact:

If IPv6 is disabled through `sysctl` config, `SSH X11forwarding` may no longer function as expected. We recommend that `SSH X11forwarding` be disabled, but if required, the following will allow for `SSH X11forwarding` with IPv6 disabled through `sysctl` config:

Add the following line the `/etc/ssh/sshd_config` file:

```
AddressFamily inet
```

Run the following command to re-start the openSSH server:

```
# systemctl restart sshd
```

Audit:

Run the following commands to verify that one of the following methods has been used to disable IPv6:

IF IPv6 is disabled through the GRUB2 config:

Run the following command and verify no lines should be returned.

```
# grep "^s*linux" /boot/grub2/grub.cfg | grep -v ipv6.disable=1
```

OR

IF IPv6 is disabled through sysctl settings:

Run the following commands:

```
# sysctl net.ipv6.conf.all.disable_ipv6

net.ipv6.conf.all.disable_ipv6 = 1
# sysctl net.ipv6.conf.default.disable_ipv6

net.ipv6.conf.default.disable_ipv6 = 1
# grep -E
'^\s*net\.ipv6\.conf\.(all|default)\.disable_ipv6\s*=\s*1\b(\s+#.*)?$'
/etc/sysctl.conf /etc/sysctl.d/*.conf | cut -d: -f2

net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
```

Remediation:

Use **one** of the two following methods to disable IPv6 on the system:

To disable IPv6 through the GRUB2 config:

Edit `/etc/default/grub` and add `ipv6.disable=1` to the `GRUB_CMDLINE_LINUX` parameters:

```
GRUB_CMDLINE_LINUX="ipv6.disable=1"
```

Run the following command to update the `grub2` configuration:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

OR

To disable IPv6 through sysctl settings:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv6.conf.all.disable_ipv6=1
# sysctl -w net.ipv6.conf.default.disable_ipv6=1
# sysctl -w net.ipv6.route.flush=1
```

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> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> 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.			

3.1.2 Ensure wireless interfaces are disabled (Automated)

Profile Applicability:

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

Description:

Wireless networking is used when wired networks are unavailable.

Rationale:

If wireless is not to be used, wireless devices should 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:

```
#!/bin/bash

if command -v nmcli >/dev/null 2>&1 ; then
    if nmcli radio all | grep -Eq '\s*\S+\s+disabled\s+\S+\s+disabled\b'; then
        echo "Wireless is not enabled"
    else
        nmcli radio all
    fi
elif [ -n "$(find /sys/class/net/*/ -type d -name wireless)" ]; then
    t=0
    mname=$(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 dm in $mname; do
        if grep -Eq "^s*install\s+$dm\s+/bin/(true|false)"
/etc/modprobe.d/*.conf; then
            /bin/true
        else
            echo "$dm is not disabled"
            t=1
        fi
    done
    [ "$t" -eq 0 ] && echo "Wireless is not enabled"
else
    echo "Wireless is not enabled"
fi
```

Output should be:

```
Wireless is not enabled
```

Remediation:

Run the following script to disable any wireless interfaces:

```
#!/bin/bash

if command -v nmcli >/dev/null 2>&1 ; then
    nmcli radio all off
else
    if [ -n "$(find /sys/class/net/*/ -type d -name wireless)" ]; then
        mname=$(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 dm in $mname; do
            echo "install $dm /bin/true" >>
/etc/modprobe.d/disable_wireless.conf
        done
    fi
fi
```


References:

1. CCI-001443: The information system protects wireless access to the system using authentication of users and/or devices
2. NIST SP 800-53 :: AC-18 (1)
3. NIST SP 800-53A :: AC-18 (1).1
4. NIST SP 800-53 Revision 4 :: AC-18 (1)
5. CCI-001444: The information system protects wireless access to the system using encryption
6. NIST SP 800-53 :: AC-18 (1)
7. NIST SP 800-53A :: AC-18 (1).1
8. NIST SP 800-53 Revision 4 :: AC-18 (1)
9. CCI-002418: The information system protects the confidentiality and/or integrity of transmitted information.
10. NIST SP 800-53 Revision 4 :: SC-8

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204634
Rule ID: SV-204634r603261_rule
STIG ID: RHEL-07-041010
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> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	15.4 <u>Disable Wireless Access on Devices if Not Required</u> Disable wireless access on devices that do not have a business purpose for wireless access.			
v7	15.5 <u>Limit Wireless Access on Client Devices</u> 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.			

3.2 Network Parameters (Host Only)

The following network parameters are intended for use if the system is to act as a host only. A system is considered host only if the system has a single interface, or has multiple interfaces but will not be configured as a router.

Note:

- sysctl settings are defined through files in `/usr/lib/sysctl.d/`, `/run/sysctl.d/`, and `/etc/sysctl.d/`.
- Files must have the the ".conf" extension.
- Vendors settings live in `/usr/lib/sysctl.d/`
- 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 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`

3.2.1 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 the flags 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.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.ip_forward

net.ipv4.ip_forward = 0
# grep -E -s "^s*net\.ipv4\.ip_forward\s*=\s*1" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

No value should be returned
```

If IPv6 is enabled:

Run the following commands and verify output matches:

```
# sysctl net.ipv6.conf.all.forwarding

net.ipv6.conf.all.forwarding = 0
# grep -E -s "^s*net\.ipv6\.conf\.all\.forwarding\s*=\s*1" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

No value should be returned
```

OR

Verify that IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

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

ipv6_chk()
{
    passing=""
    grubfile="$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o
-name 'grub.cfg' \) \
    -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;)"
    ! grep -P -- "^h*(kernelopts=|linux|kernel)" "$grubfile" | grep -vq --
ipv6.disable=1 && passing="true"
    grep -Pq -- "\s*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*?)?$" \
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    grep -Pq -- "\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*?)?$"
\
    /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    sysctl net.ipv6.conf.all.disable_ipv6 | \
    grep -Pq -- "\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*?)?$" &&
\
    sysctl net.ipv6.conf.default.disable_ipv6 | \
    grep -Pq -- "\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*?)?$"
&& passing="true"
    if [ "$passing" = true ] ; then
        echo -e "\nIPv6 is disabled on the system\n"
    else
        echo -e "\nIPv6 is enabled on the system\n"
    fi
}
ipv6_chk
```

Remediation:

Run the following commands to restore the default parameters and set the active kernel parameters:

```
# grep -Els "\s*net\.ipv4\.ip_forward\s*=\s*1" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | while
read filename; do sed -ri "s/^\s*(net\.ipv4\.ip_forward\s*) (=) (\s*\S+\b).*$/#
*REMOVED* \1/" $filename; done; sysctl -w net.ipv4.ip_forward=0; sysctl -w
net.ipv4.route.flush=1
# grep -Els "\s*net\.ipv6\.conf\.all\.forwarding\s*=\s*1" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | while
read filename; do sed -ri
"s/^\s*(net\.ipv6\.conf\.all\.forwarding\s*) (=) (\s*\S+\b).*$/#
*REMOVED* \1/"
$filename; done; sysctl -w net.ipv6.conf.all.forwarding=0; sysctl -w
net.ipv6.route.flush=1
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204625
Rule ID: SV-204625r603261_rule
STIG ID: RHEL-07-040740
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

3.2.2 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.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.conf.all.send_redirects

net.ipv4.conf.all.send_redirects = 0
# sysctl net.ipv4.conf.default.send_redirects

net.ipv4.conf.default.send_redirects = 0
# grep "net\.ipv4\.conf\.all\.send_redirects" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

net.ipv4.conf.all.send_redirects = 0
# grep "net\.ipv4\.conf\.default\.send_redirects" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

net.ipv4.conf.default.send_redirects= 0
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
```

Run the following commands to set the active kernel parameters:

```
# 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
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204616
Rule ID: SV-204616r603261_rule
STIG ID: RHEL-07-040650
Severity: CAT II

Vul ID: V-204617
Rule ID: SV-204617r603261_rule
STIG ID: RHEL-07-040660
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process 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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.			

3.3 Network Parameters (Host and Router)

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.

Note:

- sysctl settings are defined through files in `/usr/lib/sysctl.d/`, `/run/sysctl.d/`, and `/etc/sysctl.d/`.
- Files must have the the ".conf" extension.
- Vendors settings live in `/usr/lib/sysctl.d/`
- 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 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`

3.3.1 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 commands and verify output matches:

```
# sysctl net.ipv4.conf.all.accept_source_route

net.ipv4.conf.all.accept_source_route = 0
# sysctl net.ipv4.conf.default.accept_source_route

net.ipv4.conf.default.accept_source_route = 0
# grep "net\.ipv4\.conf\.all\.accept_source_route" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

net.ipv4.conf.all.accept_source_route= 0
# grep "net\.ipv4\.conf\.default\.accept_source_route" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

net.ipv4.conf.default.accept_source_route= 0
```

IF IPv6 is enabled:

Run the following commands and verify output matches:

```
# sysctl net.ipv6.conf.all.accept_source_route

net.ipv6.conf.all.accept_source_route = 0
# sysctl net.ipv6.conf.default.accept_source_route

net.ipv6.conf.default.accept_source_route = 0
# grep "net\.ipv6\.conf\.all\.accept_source_route" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

net.ipv4.conf.all.accept_source_route= 0
# grep "net\.ipv6\.conf\.default\.accept_source_route" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

net.ipv6.conf.default.accept_source_route= 0
```

OR

Verify that IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

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

ipv6_chk()
{
    passing=""
    grubfile="$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o
-name 'grub.cfg' \) \
    -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;)"
    ! grep -P -- "^h*(kernelopts=|linux|kernel)" "$grubfile" | grep -vq --
ipv6.disable=1 && passing="true"
    grep -Pq -- "^s*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*?)?$" \
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    grep -Pq -- "^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*?)?$"
\
    /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    sysctl net.ipv6.conf.all.disable_ipv6 | \
    grep -Pq -- "^h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*?)?$" &&
\
    sysctl net.ipv6.conf.default.disable_ipv6 | \
    grep -Pq -- "^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*?)?$"
&& passing="true"
    if [ "$passing" = true ] ; then
        echo -e "\nIPv6 is disabled on the system\n"
    else
        echo -e "\nIPv6 is enabled on the system\n"
    fi
}
ipv6_chk
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
```

Run the following commands to set the active kernel parameters:

```
# 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 not disabled:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv6.conf.all.accept_source_route = 0
net.ipv6.conf.default.accept_source_route = 0
```

Run the following commands to set the active kernel parameters:

```
# 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
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204609
Rule ID: SV-204609r603261_rule
STIG ID: RHEL-07-040610
Severity: CAT II

Vul ID: V-204612
Rule ID: SV-204612r603261_rule
STIG ID: RHEL-07-040620
Severity: CAT II

Vul ID: V-204630
Rule ID: SV-204630r603261_rule
STIG ID: RHEL-07-040830
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

3.3.2 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. By setting `net.ipv4.conf.all.accept_redirects` and `net.ipv6.conf.all.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.

Rationale:

Attackers could use bogus ICMP redirect messages to maliciously alter the system routing tables and get them to send packets to incorrect networks and allow your system packets to be captured.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.conf.all.accept_redirects

net.ipv4.conf.all.accept_redirects = 0
# sysctl net.ipv4.conf.default.accept_redirects

net.ipv4.conf.default.accept_redirects = 0
# grep "net\.ipv4\.conf\.all\.accept_redirects" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

net.ipv4.conf.all.accept_redirects= 0
# grep "net\.ipv4\.conf\.default\.accept_redirects" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

net.ipv4.conf.default.accept_redirects= 0
```

IF IPv6 is not disabled:

Run the following commands and verify output matches:

```
# sysctl net.ipv6.conf.all.accept_redirects

net.ipv6.conf.all.accept_redirects = 0
# sysctl net.ipv6.conf.default.accept_redirects

net.ipv6.conf.default.accept_redirects = 0
# grep "net\.ipv6\.conf\.all\.accept_redirects" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

net.ipv6.conf.all.accept_redirects= 0
# grep "net\.ipv6\.conf\.default\.accept_redirects" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

net.ipv6.conf.default.accept_redirects= 0
```

OR verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

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

ipv6_chk()
{
    passing=""
    grubfile="$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o
-name 'grub.cfg' \) \
    -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;)"
    ! grep -P -- "^h*(kernelopts=|linux|kernel)" "$grubfile" | grep -vq --
ipv6.disable=1 && passing="true"
    grep -Pq -- "^h*net\.ipv6\.conf\.all\.disable_ipv6h*=\h*1\h*(#.*?)?$" \
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    grep -Pq -- "^h*net\.ipv6\.conf\.default\.disable_ipv6h*=\h*1\h*(#.*?)?$" \
\
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    sysctl net.ipv6.conf.all.disable_ipv6 | \
    grep -Pq -- "^h*net\.ipv6\.conf\.all\.disable_ipv6h*=\h*1\h*(#.*?)?$" &&
\
    sysctl net.ipv6.conf.default.disable_ipv6 | \
    grep -Pq -- "^h*net\.ipv6\.conf\.default\.disable_ipv6h*=\h*1\h*(#.*?)?$"
&& passing="true"
    if [ "$passing" = true ] ; then
        echo -e "\nIPv6 is disabled on the system\n"
    else
        echo -e "\nIPv6 is enabled on the system\n"
    fi
}
ipv6_chk
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
```

Run the following commands to set the active kernel parameters:

```
# 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 not disabled

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv6.conf.all.accept_redirects = 0
net.ipv6.conf.default.accept_redirects = 0
```

Run the following commands to set the active kernel parameters:

```
# 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
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204614
Rule ID: SV-204614r603261_rule
STIG ID: RHEL-07-040640
Severity: CAT II

Vul ID: V-204615
Rule ID: SV-204615r603261_rule
STIG ID: RHEL-07-040641
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

3.3.3 Ensure network interfaces are not in promiscuous mode (Manual)

Profile Applicability:

- STIG

Description:

Network interfaces configured on the operating system 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 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 and documented, refer to the remediation procedure below.

Remediation:

Configure network interfaces to turn off promiscuous mode unless approved 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. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204618
Rule ID: SV-204618r603261_rule
STIG ID: RHEL-07-040670
Severity: CAT II

3.3.4 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` to 0 protects the system from routing table updates by possibly compromised known gateways.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.conf.all.secure_redirects

net.ipv4.conf.all.secure_redirects = 0
# sysctl net.ipv4.conf.default.secure_redirects

net.ipv4.conf.default.secure_redirects = 0
# grep "net\.ipv4\.conf\.all\.secure_redirects" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

net.ipv4.conf.all.secure_redirects= 0
# grep "net\.ipv4\.conf\.default\.secure_redirects" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

net.ipv4.conf.default.secure_redirects= 0
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
```

Run the following commands to set the active kernel parameters:

```
# 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
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

3.3.5 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:

Enabling this feature and logging these packets allows an administrator to investigate the possibility that an attacker is sending spoofed packets to their system.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.conf.all.log_martians

net.ipv4.conf.all.log_martians = 1
# sysctl net.ipv4.conf.default.log_martians

net.ipv4.conf.default.log_martians = 1
# grep "net\.ipv4\.conf\.all\.log_martians" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

net.ipv4.conf.all.log_martians = 1
# grep "net\.ipv4\.conf\.default\.log_martians" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

net.ipv4.conf.default.log_martians = 1
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.log_martians = 1
```

Run the following commands to set the active kernel parameters:

```
# 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
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

3.3.6 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 commands and verify output matches:

```
# sysctl net.ipv4.icmp_echo_ignore_broadcasts

net.ipv4.icmp_echo_ignore_broadcasts = 1

# grep "net\.ipv4\.icmp_echo_ignore_broadcasts" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

net.ipv4.icmp_echo_ignore_broadcasts = 1
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
# sysctl -w net.ipv4.route.flush=1
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204613
Rule ID: SV-204613r603261_rule
STIG ID: RHEL-07-040630
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process 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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.			

3.3.7 Ensure bogus ICMP responses are ignored (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Setting `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 commands and verify output matches:

```
# sysctl net.ipv4.icmp_ignore_bogus_error_responses
net.ipv4.icmp_ignore_bogus_error_responses = 1

# grep "net.ipv4.icmp ignore bogus error responses" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf
net.ipv4.icmp_ignore_bogus_error_responses = 1
```

Remediation:

Set the following parameter in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.icmp_ignore_bogus_error_responses = 1
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1
# sysctl -w net.ipv4.route.flush=1
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

3.3.8 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 these flags 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.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.conf.all.rp_filter

net.ipv4.conf.all.rp_filter = 1
# sysctl net.ipv4.conf.default.rp_filter

net.ipv4.conf.default.rp_filter = 1
# grep "net\.ipv4\.conf\.all\.rp_filter" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

net.ipv4.conf.all.rp_filter = 1
# grep "net\.ipv4\.conf\.default\.rp_filter" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

net.ipv4.conf.default.rp_filter = 1
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
```

Run the following commands to set the active kernel parameters:

```
# 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
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204610
Rule ID: SV-204610r603261_rule
STIG ID: RHEL-07-040611
Severity: CAT II

Vul ID: V-204611
Rule ID: SV-204611r603261_rule
STIG ID: RHEL-07-040612
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

3.3.9 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. SYN cookies allow the system to keep accepting valid connections, even if under a denial of service attack.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.tcp_syncookies

net.ipv4.tcp_syncookies = 1

# grep "net\.ipv4\.tcp_syncookies" /etc/sysctl.conf /etc/sysctl.d/*.conf
/usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

net.ipv4.tcp_syncookies = 1
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.tcp_syncookies = 1
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.tcp_syncookies=1
# sysctl -w net.ipv4.route.flush=1
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

3.3.10 Ensure IPv6 router advertisements are not accepted (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

This setting disables the system's ability to accept IPv6 router 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.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv6.conf.all.accept_ra
net.ipv6.conf.all.accept_ra = 0
# sysctl net.ipv6.conf.default.accept_ra
net.ipv6.conf.default.accept_ra = 0
# grep "net\.ipv6\.conf\.all\.accept_ra" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

net.ipv6.conf.all.accept_ra = 0
# grep "net\.ipv6\.conf\.default\.accept_ra" /etc/sysctl.conf
/etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf

net.ipv6.conf.default.accept_ra = 0
```

OR Verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.


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

ipv6_chk()
{
    passing=""
    grubfile="$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o
-name 'grub.cfg' \) \
    -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;)"
    ! grep -P -- "^h*(kernelopts=|linux|kernel)" "$grubfile" | grep -vq --
ipv6.disable=1 && passing="true"
    grep -Pq -- "^s*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*?)?$" \
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    grep -Pq -- "^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*?)?$"
\
    /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    sysctl net.ipv6.conf.all.disable_ipv6 | \
    grep -Pq -- "^h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*?)?$" &&
\
    sysctl net.ipv6.conf.default.disable_ipv6 | \
    grep -Pq -- "^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*?)?$"
&& passing="true"
    if [ "$passing" = true ] ; then
        echo -e "\nIPv6 is disabled on the system\n"
    else
        echo -e "\nIPv6 is enabled on the system\n"
    fi
}
ipv6_chk
```

Remediation:

IF IPv6 is enabled:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv6.conf.all.accept_ra = 0
net.ipv6.conf.default.accept_ra = 0
```

Run the following commands to set the active kernel parameters:

```
# 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
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

3.4 Uncommon Network Protocols

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.

3.4.1 Ensure DCCP is disabled (Automated)

Profile Applicability:

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

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 commands and verify the output is as indicated:

```
# modprobe -n -v dccp
install /bin/true

# lsmod | grep dccp
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

Example: `vim /etc/modprobe.d/dccp.conf`

Add the following line:

```
install dccp /bin/true
```

References:

1. CCI: CCI-001958: The information system authenticates an organization defined list of specific and/or types of devices before establishing a local, remote, or network connection.
2. NIST SP 800-53 Revision 4 :: IA-3

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204450
Rule ID: SV-204450r603261_rule
STIG ID: RHEL-07-020101
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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

3.4.2 Ensure SCTP is disabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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 commands and verify the output is as indicated:

```
# modprobe -n -v sctp
install /bin/true

# lsmod | grep sctp
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

Example: `vim /etc/modprobe.d/sctp.conf`

Add the following line:

```
install sctp /bin/true
```

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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

3.5 Firewall Configuration

A firewall 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:

- Netfilter - A set of hooks inside the Linux kernel that allows kernel modules to register callback functions with the network stack. A registered callback function is then called back for every packet that traverses the respective hook within the network stack. Includes the `ip_tables`, `ip6_tables`, `arp_tables`, and `ebtables` kernel modules. These modules are some of the significant parts of the Netfilter hook system.
- 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. **Is available in Linux kernels 3.13 and newer.**

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 iptables 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.
- nftables - Includes the nft utility for configuration of the nftables subsystem of the Linux kernel
- iptables - Includes the iptables, ip6tables, arptables and ebtables utilities for configuration Netfilter and the `ip_tables`, `ip6_tables`, `arp_tables`, and `ebtables` kernel modules.

Note:

- *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.*

3.5.1 Configure firewalld

If nftables or iptables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.

firewalld (Dynamic Firewall Manager) provides a dynamically managed firewall with support for network/firewall “zones” to assign a level of trust to a network and its associated connections, interfaces or sources. It has support for IPv4, IPv6, Ethernet bridges and also for IPSet firewall settings. There is a separation of the runtime and permanent configuration options. It also provides an interface for services or applications to add iptables, ip6tables and ebtables rules directly. This interface can also be used by advanced users.

In the v0.6.0 release, firewalld gained support for using nftables as a firewall back-end.

Note: Configuration of a live system's firewall directly over a remote connection will often result in being locked out.

3.5.1.1 Ensure firewalld is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

firewalld is a firewall management tool for Linux operating systems. It provides firewall features by acting as a front-end for the Linux kernel's netfilter framework via the iptables backend or provides firewall features by acting as a front-end for the Linux kernel's netfilter framework via the nftables utility.

firewalld replaces iptables as the default firewall management tool. Use the firewalld utility to configure a firewall for less complex firewalls. The utility is easy to use and covers the typical use cases scenario. FirewallD supports both IPv4 and IPv6 networks and can administer separate firewall zones with varying degrees of trust as defined in zone profiles.

Note: 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.

Rationale:

A firewall utility is required to configure the Linux kernel's netfilter framework via the iptables or nftables back-end.

The Linux kernel's netfilter framework host-based firewall can protect against threats originating from within a corporate network to include malicious mobile code and poorly configured software on a host.

*Note: Only **one** firewall utility should be installed and configured. FirewallD is dependent on the iptables package.*

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 FirewallD and iptables are installed:

```
# rpm -q firewalld iptables  
  
firewalld-<version>  
iptables-<version>
```

Remediation:

Run the following command to install FirewallD and iptables:

```
# yum install firewalld iptables
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.1.2 Ensure iptables-services not installed with firewalld (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `iptables-services` package contains the `iptables.service` and `ip6tables.service`. These services allow for management of the Host Based Firewall provided by the `iptables` package.

Rationale:

`iptables.service` and `ip6tables.service` are still supported and can be installed with the `iptables-services` package. Running both `firewalld` and the services included in the `iptables-services` package may lead to conflict.

Impact:

Running both `firewalld` and `iptables/ip6tables` service may lead to conflict.

Audit:

Run the following commands to verify that the `iptables-services` package is not installed

```
# rpm -q iptables-services
package iptables-services is not installed
```

Remediation:

Run the following commands to stop the services included in the `iptables-services` package and remove the `iptables-services` package

```
# systemctl stop iptables
# systemctl stop ip6tables
# yum remove iptables-services
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.4 Implement and Manage a Firewall on Servers</u> 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	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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>9.4 Apply Host-based Firewalls or Port Filtering</u> 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.			

3.5.1.3 Ensure nftables either not installed or masked with firewalld (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames and is the successor to iptables.

_Note: Support for using nftables as the back-end for firewalld was added in release v0.6.0. In Fedora 19 Linux derivatives, firewalld utilizes iptables as its back-end by default.

Rationale:

Running both firewalld and nftables may lead to conflict.

Note: firewalld may configured as the front-end to nftables. If this case, nftables should be stopped and masked instead of removed.

Audit:

Run the following command to verify that nftables is not installed:

```
# rpm -q nftables
package nftables is not installed
```

OR

Run the following commands to verify that nftables is stopped:

```
# systemctl status nftables | grep "Active: " | grep -E " active
\((running|exited)\) "
```

No output should be returned

Run the following command to verify nftables.service is masked:

```
# systemctl is-enabled nftables
masked
```

Remediation:

Run the following command to remove `nftables`:

```
# yum remove nftables
```

OR

Run the following command to stop and mask `nftables`:

```
systemctl --now mask nftables
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> 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.			

3.5.1.4 Ensure firewalld service enabled and running (Automated)

Profile Applicability:

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

Description:

`firewalld.service` enables the enforcement of firewall rules configured through `firewalld`

Rationale:

Ensure that the `firewalld.service` is enabled and running to enforce firewall rules configured through `firewalld`

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 unmask `firewalld`

```
# systemctl unmask firewalld
```

Run the following command to enable and start `firewalld`

```
# systemctl --now enable firewalld
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204604
Rule ID: SV-204604r603261_rule
STIG ID: RHEL-07-040520
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> 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> 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.			

3.5.1.5 Ensure firewalld default zone is set (Automated)

Profile Applicability:

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

Description:

A firewall zone defines the trust level for a connection, interface or source address binding. This is a one to many relation, which means that a connection, interface or source can only be part of one zone, but a zone can be used for many network connections, interfaces and sources.

- The default zone is the zone that is used for everything that is not explicitly bound/assigned to another zone.
- If no zone assigned to a connection, interface or source, only the default zone is used.
- The default zone is not always listed as being used for an interface or source as it will be used for it either way. This depends on the manager of the interfaces.

Connections handled by NetworkManager are listed as NetworkManager requests to add the zone binding for the interface used by the connection. Also interfaces under control of the network service are listed also because the service requests it.

Note:

- *A firewalld zone configuration file contains the information for a zone.*
 - *These are the zone description, services, ports, protocols, icmp-blocks, masquerade, forward-ports and rich language rules in an XML file format.*
 - *The file name has to be `zone_name.xml` where length of `zone_name` is currently limited to 17 chars.*
- *NetworkManager binds interfaces to zones automatically*

Rationale:

Because the default zone is the zone that is used for everything that is not explicitly bound/assigned to another zone, it is important for the default zone to set

Audit:

Run the following command and verify that the default zone adheres to company policy:

```
# firewall-cmd --get-default-zone
```

Remediation:

Run the following command to set the default zone:

```
# firewall-cmd --set-default-zone=<NAME_OF_ZONE>
```

Example:

```
# firewall-cmd --set-default-zone=public
```

References:

1. <https://firewalld.org/documentation>
2. <https://firewalld.org/documentation/man-pages/firewalld.zone>
3. CCI-000366: The organization implements the security configuration settings
4. NIST SP 800-53 :: CM-6 b
5. NIST SP 800-53A :: CM-6.1 (iv)
6. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204628
Rule ID: SV-204628r603261_rule
STIG ID: RHEL-07-040810
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> 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> 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.			

3.5.1.6 Ensure network interfaces are assigned to appropriate zone (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

firewall zones define the trust level of network connections or interfaces.

Rationale:

A network interface not assigned to the appropriate zone can allow unexpected or undesired network traffic to be accepted on the interface.

Impact:

Changing firewall settings while connected over network can result in being locked out of the system.

Audit:

Run the following and verify that the interface(s) follow site policy for zone assignment

```
# find /sys/class/net/* -maxdepth 1 | awk -F"/" '{print $NF}' | while read -r netint; do [ "$netint" != "lo" ] && firewall-cmd --get-active-zones | grep -B1 $netint; done
```

Example output:

```
<custom zone>  
eth0
```

Remediation:

Run the following command to assign an interface to the appropriate zone.

```
# firewall-cmd --zone=<Zone NAME> --change-interface=<INTERFACE NAME>
```

Example:

```
# firewall-cmd --zone=customzone --change-interface=eth0
```

Default Value:

default zone defined in the firewalld configuration

References:

1. <https://firewalld.org/documentation/zone/connections-interfaces-and-sources.html>

Additional Information:

The firewall in the Linux kernel is not able to handle network connections with the name shown by NetworkManager, it can only handle the network interfaces used by the connection. Because of this NetworkManager tells firewalld to assign the network interface that is used for this connection to the zone defined in the configuration of that connection. This assignment happens before the interface is used. The configuration of the connection can either be the NetworkManager configuration or also an `ifcfg`.

Example: If the zone is not set in the configuration file, the interfaces will be assigned to the default zone defined in the firewalld configuration. If a connection has more than one interface, all of them will be supplied to firewalld. Also changes in the names of interfaces will be handled by NetworkManager and supplied to firewalld.

If the zone is not set in the configuration file, the interfaces will be assigned to the default zone defined in the firewalld configuration

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers 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 Apply Host-based Firewalls or Port Filtering 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.			

3.5.1.7 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.

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.

```
# firewall-cmd --get-active-zones | awk '!/:/ {print $1}' | while read ZN; do  
firewall-cmd --list-all --zone=$ZN; done
```

Remediation:

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. firewall.service(5)
2. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/securing_networks/using-and-configuring-firewalls_securing-networks

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers 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 Apply Host-based Firewalls or Port Filtering 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.			

3.5.2 Configure nftables

If firewalld or iptables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames and is the successor to iptables. The biggest change with the successor nftables is its simplicity. With iptables, we have to configure every single rule and use the syntax which can be compared with normal commands. With nftables, the simpler syntax, much like BPF (Berkely Packet Filter) means shorter lines and less repetition. Support for nftables should also be compiled into the kernel, together with the related nftables modules. It is available in Linux kernels ≥ 3.13 . **Please ensure that your kernel supports nftables before choosing this option.**

This section broadly assumes starting with an empty nftables firewall ruleset (established by flushing the rules with `nft flush ruleset`). Remediation steps included only affect the live system, you will also need to configure your default firewall configuration to apply on boot. **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: *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.*

The following will implement the firewall rules of this section and 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) needs to be updated to only allow systems requiring ssh connectivity to connect, as per site policy.

Save the script bellow as `/etc/nftables/nftables.rules`

```
#!/sbin/nft -f

# 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 {
    # Base chain for input hook named input (Filters inbound network packets)
    chain input {
        type filter hook input priority 0; policy drop;

        # Ensure loopback traffic is configured
        iif "lo" accept
        ip saddr 127.0.0.0/8 counter packets 0 bytes 0 drop
        ip6 saddr ::1 counter packets 0 bytes 0 drop

        # Ensure established connections are configured
        ip protocol tcp ct state established accept
        ip protocol udp ct state established accept
        ip protocol icmp ct state established accept

        # Accept port 22(SSH) traffic from anywhere
        tcp dport ssh accept

        # Accept ICMP and IGMP from anywhere
        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
        ip protocol igmp accept
    }

    # Base chain for hook forward named forward (Filters forwarded network
packets)
    chain forward {
        type filter hook forward priority 0; policy drop;
    }

    # Base chain for hook output named output (Filters outbound network packets)
    chain output {
        type filter hook output priority 0; policy drop;
        # Ensure outbound and established connections are configured
        ip protocol tcp ct state established,related,new accept
        ip protocol udp ct state established,related,new accept
        ip protocol icmp ct state established,related,new accept
    }
}
```

Run the following command to load the file into nftables

```
# nft -f /etc/nftables/nftables.rules
```

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"
```

3.5.2.1 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.

Note:

- *nftables is available in Linux kernel 3.13 and newer.*
- *Only **one** firewall utility should be installed and configured.*

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`

```
# yum install nftables
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.2.2 Ensure firewalld is either not installed or masked with nftables (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

firewalld (Dynamic Firewall Manager) provides a dynamically managed firewall with support for network/firewall “zones” to assign a level of trust to a network and its associated connections, interfaces or sources. It has support for IPv4, IPv6, Ethernet bridges and also for IPSet firewall settings. There is a separation of the runtime and permanent configuration options.

Rationale:

Running both `nftables.service` and `firewalld.service` may lead to conflict and unexpected results.

Audit:

Run the following command to verify that `firewalld` is not installed:

```
# rpm -q firewalld  
package firewalld is not installed
```

OR

Run the following command to verify that FirewallD is not running

```
command -v firewall-cmd >/dev/null && firewall-cmd --state | grep 'running'  
not running
```

Run the following command to verify that FirewallD is masked

```
# systemctl is-enabled firewalld  
masked
```

Remediation:

Run the following command to remove `firewalld`

```
# yum remove firewalld
```

OR

Run the following command to stop and mask `firewalld`

```
# systemctl --now mask firewalld
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> 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.			

3.5.2.3 Ensure iptables-services not installed with nftables (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `iptables-services` package contains the `iptables.service` and `ip6tables.service`. These services allow for management of the Host Based Firewall provided by the `iptables` package.

Rationale:

`iptables.service` and `ip6tables.service` are still supported and can be installed with the `iptables-services` package. Running both `nftables` and the services included in the `iptables-services` package may lead to conflict.

Audit:

Run the following commands to verify that the `iptables-services` package is not installed

```
# rpm -q iptables-services  
package iptables-services is not installed
```

Remediation:

Run the following commands to stop the services included in the `iptables-services` package and remove the `iptables-services` package

```
# systemctl stop iptables  
# systemctl stop ip6tables  
# yum remove iptables-services
```


CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.4 Implement and Manage a Firewall on Servers</u> 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	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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>9.4 Apply Host-based Firewalls or Port Filtering</u> 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.			

3.5.2.4 Ensure iptables are flushed with nftables (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

nftables is a replacement for iptables, ip6tables, ebtables and arptables

Rationale:

It is possible to mix iptables and nftables. However, this increases complexity and also the chance to introduce errors. For simplicity flush out all iptables rules, and ensure it is not loaded

Audit:

Run the following commands to ensure not iptables rules exist

For iptables:

```
# iptables -L  
No rules should be returned
```

For ip6tables:

```
# ip6tables -L  
No rules should be returned
```

Remediation:

Run the following commands to flush iptables:

For iptables:

```
# iptables -F
```

For ip6tables:

```
# ip6tables -F
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.2.5 Ensure an nftables table exists (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Tables hold chains. Each table only has one address family and only applies to packets of this family. Tables can have one of five families.

Rationale:

nftables doesn't have any default tables. Without a table being build, nftables will not filter network traffic.

Impact:

Adding rules to a running nftables can cause loss of connectivity to the system

Audit:

Run the following command to verify that a nftables table exists:

```
# nft list tables
```

Return should include a list of nftables:

Example:

```
table inet filter
```

Remediation:

Run the following command to create a table in nftables

```
# nft create table inet <table name>
```

Example:

```
# nft create table inet filter
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.2.6 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.

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 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:

Run the following commands and verify that base chains exist for INPUT, FORWARD, and OUTPUT.

```
# nft list ruleset | grep 'hook input'
type filter hook input priority 0;
# nft list ruleset | grep 'hook forward'
type filter hook forward priority 0;
# nft list ruleset | grep 'hook output'
type filter hook output priority 0;
```

Remediation:

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 \;  
}
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.2.7 Ensure nftables 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 commands to verify that the loopback interface is configured:

```
# nft list ruleset | awk '/hook input/,/}/' | grep 'iif "lo" accept'
iif "lo" accept
# nft list ruleset | awk '/hook input/,/}/' | grep 'ip saddr'
ip saddr 127.0.0.0/8 counter packets 0 bytes 0 drop
```

IF IPv6 is enabled, run the following command to verify that the IPv6 loopback interface is configured:

```
# nft list ruleset | awk '/hook input/,/}/' | grep 'ip6 saddr'
ip6 saddr ::1 counter packets 0 bytes 0 drop
```

OR

Verify that IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.


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

ipv6_chk()
{
    passing=""
    grubfile="$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o
-name 'grub.cfg' \) \
    -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;)"
    ! grep -P -- "^h*(kernelopts=|linux|kernel)" "$grubfile" | grep -vq --
ipv6.disable=1 && passing="true"
    grep -Pq -- "^s*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*?)?$" \
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    grep -Pq -- "^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*?)?$"
\
    /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    sysctl net.ipv6.conf.all.disable_ipv6 | \
    grep -Pq -- "^h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*?)?$" &&
\
    sysctl net.ipv6.conf.default.disable_ipv6 | \
    grep -Pq -- "^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*?)?$"
&& passing="true"
    if [ "$passing" = true ] ; then
        echo -e "\nIPv6 is disabled on the system\n"
    else
        echo -e "\nIPv6 is enabled on the system\n"
    fi
}
ipv6_chk
```

Remediation:

Run the following commands to implement the loopback rules:

```
# nft add rule inet filter input iif lo accept
# nft create rule inet filter input ip saddr 127.0.0.0/8 counter drop
```

IF IPv6 is enabled:

Run the following command to implement the IPv6 loopback rules:

```
# nft add rule inet filter input ip6 saddr ::1 counter drop
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.2.8 Ensure nftables outbound and 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 new outbound and established connections, all packets will be dropped by the default policy preventing network usage.

Audit:

Run the following commands and verify all rules for established incoming connections match site policy: site policy:

```
# nft list ruleset | awk '/hook input/,/}/' | grep -E 'ip protocol (tcp|udp|icmp) 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
```

Run the following command and verify all rules for new and established outbound connections match site policy

```
# nft list ruleset | awk '/hook output/,/}/' | grep -E 'ip protocol (tcp|udp|icmp) ct state'
```

Output should be similar to:

```
ip protocol tcp ct state established,related,new accept
ip protocol udp ct state established,related,new accept
ip protocol icmp ct state established,related,new accept
```

Remediation:

Configure nftables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

```
# nft add rule inet filter input ip protocol tcp ct state established accept
# nft add rule inet filter input ip protocol udp ct state established accept
# nft add rule inet filter input ip protocol icmp ct state established accept
# nft add rule inet filter output ip protocol tcp ct state
new,related,established accept
# nft add rule inet filter output ip protocol udp ct state
new,related,established accept
# nft add rule inet filter output ip protocol icmp ct state
new,related,established accept
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.2.9 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 white list acceptable usage than to black list 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:

Run the following commands and verify that base chains contain a policy of `DROP`.

```
# nft list ruleset | grep 'hook input'
type filter hook input priority 0; policy drop;
# nft list ruleset | grep 'hook forward'
type filter hook forward priority 0; policy drop;
# nft list ruleset | grep 'hook output'
type filter hook output priority 0; policy drop;
```

Remediation:

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 \; }
# nft chain inet filter output { policy drop \; }
```

Default Value:

accept

References:

1. Manual Page nft

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.2.10 Ensure nftables service is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The nftables service allows for the loading of nftables rulesets during boot, or starting on the nftables service

Rationale:

The nftables service restores the nftables rules from the rules files referenced in the `/etc/sysconfig/nftables.conf` file during boot or the starting of the nftables service

Audit:

Run the following command and verify that the nftables service is enabled:

```
# systemctl is-enabled nftables
enabled
```

Remediation:

Run the following command to enable the nftables service:

```
# systemctl enable nftables
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.2.11 Ensure nftables rules are permanent (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames.

The nftables service reads the `/etc/sysconfig/nftables.conf` file for a nftables file or files to include in the nftables ruleset.

A nftables ruleset containing the input, forward, and output base chains allow network traffic to be filtered.

Rationale:

Changes made to nftables ruleset only affect the live system, you will also need to configure the nftables ruleset to apply on boot

Audit:

Run the following commands to verify that input, forward, and output base chains are configured to be applied to a nftables ruleset on boot:

Run the following command to verify the input base chain:

```
# awk '/hook input/,/}/' $(awk '$1 ~ /^s*include/ { gsub("\"","",$2);print $2 }' /etc/sysconfig/nftables.conf)
```

Output should be similar to:

```
type filter hook input priority 0; policy drop;

# Ensure loopback traffic is configured
iif "lo" accept
ip saddr 127.0.0.0/8 counter packets 0 bytes 0 drop
ip6 saddr ::1 counter packets 0 bytes 0 drop

# Ensure established connections are configured
ip protocol tcp ct state established accept
ip protocol udp ct state established accept
ip protocol icmp ct state established accept

# Accept port 22 (SSH) traffic from anywhere
tcp dport ssh accept

# Accept ICMP and IGMP from anywhere
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
```

Note: Review the input base chain to ensure that it follows local site policy

Run the following command to verify the forward base chain:

```
# awk '/hook forward/,/}/' $(awk '$1 ~ /^s*include/ { gsub("\"","",$2);print $2 }' /etc/sysconfig/nftables.conf)
```

Output should be similar to:

```
# Base chain for hook forward named forward (Filters forwarded
network packets)
chain forward {
    type filter hook forward priority 0; policy drop;
}
```

Note: Review the forward base chain to ensure that it follows local site policy.

Run the following command to verify the forward base chain:

```
# awk '/hook output/,/}/' $(awk '$1 ~ /^s*include/ { gsub("\\"", "\"", $2); print $2 }' /etc/sysconfig/nftables.conf)
```

Output should be similar to:

```
# Base chain for hook output named output (Filters outbound network packets)
chain output {
    type filter hook output priority 0; policy drop;
    # Ensure outbound and established connections are configured
    ip protocol tcp ct state established,related,new accept
    ip protocol tcp ct state established,related,new accept
    ip protocol udp ct state established,related,new accept
    ip protocol icmp ct state established,related,new accept
}
```

Note: Review the output base chain to ensure that it follows local site policy.

Remediation:

Edit the `/etc/sysconfig/nftables.conf` file and un-comment or add a line with `include <Absolute path to nftables rules file>` for each nftables file you want included in the nftables ruleset on boot:

Example:

```
include "/etc/nftables/nftables.rules"
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.3 Configure iptables

If firewalld or nftables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.

Iptables is an application that allows a system administrator to configure the IPv4 and IPv6 tables, chains and rules provided by the Linux kernel firewall. While several methods of configuration exist this section is intended only to ensure the resulting Iptables rules are in place, not how they are configured. If IPv6 is in use in your environment, similar settings should be applied to the IP6tables as well.

Note: 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.

3.5.3.1 Configure iptables software

This section provides guidance for installing, enabling, removing, and disabling software packages necessary for using IPTables as the method for configuring and maintaining a Host Based Firewall on the system.

Note: *Using more than one method to configure and maintain a Host Based Firewall can cause unexpected results. If FirewallD or NFTables are being used for configuration and maintenance, this section should be skipped and the guidance in their respective section followed.*

3.5.3.1.1 Ensure iptables packages are installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

iptables is a utility program that allows a system administrator to configure the tables provided by the Linux kernel firewall, implemented as different Netfilter modules, and the chains and rules it stores. Different kernel modules and programs are used for different protocols; iptables applies to IPv4, ip6tables to IPv6, arptables to ARP, and ebtables to Ethernet frames.

Rationale:

A method of configuring and maintaining firewall rules is necessary to configure a Host Based Firewall.

Audit:

Run the following command to verify that iptables and iptables-services are installed:

```
rpm -q iptables iptables-services  
  
iptables-<version>  
iptables-services-<version>
```

Remediation:

Run the following command to install iptables and iptables-services

```
# yum install iptables iptables-services
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.3.1.2 Ensure nftables is not installed with iptables (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames and is the successor to iptables.

Rationale:

Running both `iptables` and `nftables` may lead to conflict.

Audit:

Run the following command to verify that nftables is not installed:

```
# rpm -q nftables  
package nftables is not installed
```

Remediation:

Run the following command to remove `nftables`:

```
# yum remove nftables
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.4 Implement and Manage a Firewall on Servers</u> 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	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 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>9.4 Apply Host-based Firewalls or Port Filtering</u> 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.			

3.5.3.1.3 Ensure firewalld is either not installed or masked with iptables (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

firewalld (Dynamic Firewall Manager) provides a dynamically managed firewall with support for network/firewall “zones” to assign a level of trust to a network and its associated connections, interfaces or sources. It has support for IPv4, IPv6, Ethernet bridges and also for IPSet firewall settings. There is a separation of the runtime and permanent configuration options.

Rationale:

Running `iptables.service` and/or `ip6tables.service` with `firewalld.service` may lead to conflict and unexpected results.

Audit:

Run the following command to verify that `firewalld` is not installed:

```
# rpm -q firewalld  
package firewalld is not installed
```

OR

Run the following commands to verify that `firewalld` is stopped and masked

```
# systemctl status firewalld | grep "Active: " | grep -v "active (running) "  
No output should be returned  
# systemctl is-enabled firewalld  
masked
```

Remediation:

Run the following command to remove `firewalld`

```
# yum remove firewalld
```

OR

Run the following command to stop and mask `firewalld`

```
# systemctl --now mask firewalld
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> 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.			

3.5.3.2 Configure IPv4 iptables

IPTables is used to set up, maintain, and inspect the tables of IP packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains.

Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a 'target', which may be a jump to a user-defined chain in the same table.

Note:

- *This section broadly assumes starting with an empty IPTables firewall ruleset (established by flushing the rules with iptables -F).*
- *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.*

The following script will implement the firewall rules of this section and open port 22(ssh) from anywhere. *This needs to be updated to only allow systems requiring ssh connectivity to connect as per site policy.*

```
#!/bin/bash

# Flush IPtables rules
iptables -F

# Ensure default deny firewall policy
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# Ensure loopback traffic is configured
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
iptables -A INPUT -s 127.0.0.0/8 -j DROP

# Ensure outbound and established connections are configured
iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT

# Open inbound ssh(tcp port 22) connections
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

3.5.3.2.1 Ensure iptables 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 (127.0.0.0/8).

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 (127.0.0.0/8) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Note: Changing firewall settings while connected over network can result in being locked out of the system.

Audit:

Run the following commands and verify output includes the listed rules in order (packet and byte counts may differ):

```
# iptables -L INPUT -v -n
Chain INPUT (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source
destination
    0     0 ACCEPT     all  --  lo      *       0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.0/8
                                     0.0.0.0/0

# iptables -L OUTPUT -v -n
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source
destination
    0     0 ACCEPT     all  --  *      lo      0.0.0.0/0
                                     0.0.0.0/0
```

Remediation:

Run the following commands to implement the loopback rules:

```
# iptables -A INPUT -i lo -j ACCEPT
# iptables -A OUTPUT -o lo -j ACCEPT
# iptables -A INPUT -s 127.0.0.0/8 -j DROP
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.3.2.2 Ensure iptables outbound and 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 new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

Note: Changing firewall settings while connected over network can result in being locked out of the system.

Audit:

Run the following command and verify all rules for new outbound, and established connections match site policy:

```
# iptables -L -v -n
```

Remediation:

Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

```
# iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
# iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
# iptables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.3.2.3 Ensure iptables rules exist for all open ports (Automated)

Profile Applicability:

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

Description:

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

Rationale:

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

Note:

- *Changing firewall settings while connected over network can result in being locked out of the system.*
- *The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy.*

Audit:

Run the following command to determine open ports:

```
# ss -4tuln
```

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer
Address:Port					
udp	UNCONN	0	0	*:68	
:					
udp	UNCONN	0	0	*:123	
:					
tcp	LISTEN	0	128	*:22	
:					

Run the following command to determine firewall rules:

```
# iptables -L INPUT -v -n
```

Chain INPUT (policy DROP 0 packets, 0 bytes)	pkts	bytes	target	prot	opt	in	out	source	destination
	0	0	ACCEPT	all	--	lo	*	0.0.0.0/0	0.0.0.0/0
	0	0	DROP	all	--	*	*	127.0.0.0/8	0.0.0.0/0
	0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0

```
tcp dpt:22 state NEW
```

Verify all open ports listening on non-localhost addresses have at least one firewall rule.

Note: The last line identified by the "tcp dpt:22 state NEW" identifies it as a firewall rule for new connections on tcp port 22.

Remediation:

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:

```
# iptables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j ACCEPT
```

References:

1. CCI-000382: The organization configures the information system to prohibit or restrict the use of organization defined functions, ports, protocols, and/or services
2. NIST SP 800-53 :: CM-7
3. NIST SP 800-53A :: CM-7.1 (iii)
4. NIST SP 800-53 Revision 4 :: CM-7 b
5. CCI-002314: The information system controls remote access methods
6. NIST SP 800-53 Revision 4 :: AC-17 (1)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204577
Rule ID: SV-204577r603261_rule
STIG ID: RHEL-07-040100
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers 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	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			
v7	9.4 Apply Host-based Firewalls or Port Filtering 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.			

3.5.3.2.4 Ensure iptables default deny firewall policy (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.

Rationale:

With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Note: Changing firewall settings while connected over network can result in being locked out of the system.

Audit:

Run the following command and verify that the policy for the `INPUT` , `OUTPUT` , and `FORWARD` chains is `DROP` or `REJECT` :

```
# iptables -L  
  
Chain INPUT (policy DROP)  
Chain FORWARD (policy DROP)  
Chain OUTPUT (policy DROP)
```

Remediation:

Run the following commands to implement a default DROP policy:

```
# iptables -P INPUT DROP  
# iptables -P OUTPUT DROP  
# iptables -P FORWARD DROP
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.3.2.5 Ensure iptables rules are saved (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `iptables-services` package includes the `/etc/sysconfig/iptables` file. The `iptables` rules in this file will be loaded by the `iptables.service` during boot, or when it is started or re-loaded.

Rationale:

If the `iptables` rules are not saved and a system re-boot occurs, the `iptables` rules will be lost.

Audit:

Review the file `/etc/sysconfig/iptables` and ensure it contains the complete correct rule-set.

Example: `/etc/sysconfig/iptables`

```
# sample configuration for iptables service
# you can edit this manually or use system-config-firewall
# Generated by iptables-save v1.4.21 on Wed Mar 25 14:23:37 2020
*filter
:INPUT DROP [4:463]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -s 127.0.0.0/8 -j DROP
-A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Wed Mar 25 14:23:37 2020
```

Remediation:

Run the following commands to create or update the `/etc/sysconfig/iptables` file:

Run the following command to review the current running `iptables` configuration:

```
# iptables -L
```

Output should include:

```
Chain INPUT (policy DROP)
target     prot opt source                destination
ACCEPT     all  --  anywhere              anywhere
DROP       all  --  loopback/8           anywhere
ACCEPT     tcp  --  anywhere              anywhere    state
ESTABLISHED
ACCEPT     udp  --  anywhere              anywhere    state
ESTABLISHED
ACCEPT     icmp --  anywhere              anywhere    state
ESTABLISHED
ACCEPT     tcp  --  anywhere              anywhere    tcp dpt:ssh
state NEW

Chain FORWARD (policy DROP)
target     prot opt source                destination

Chain OUTPUT (policy DROP)
target     prot opt source                destination
ACCEPT     all  --  anywhere              anywhere
ACCEPT     tcp  --  anywhere              anywhere    state
NEW,ESTABLISHED
ACCEPT     udp  --  anywhere              anywhere    state
NEW,ESTABLISHED
ACCEPT     icmp --  anywhere              anywhere    state
NEW,ESTABLISHED
```

Run the following command to save the verified running configuration to the file

`/etc/sysconfig/iptables`:

```
# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.3.2.6 Ensure iptables is enabled and running (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`iptables.service` is a utility for configuring and maintaining `iptables`.

Rationale:

`iptables.service` will load the `iptables` rules saved in the file `/etc/sysconfig/iptables` at boot, otherwise the `iptables` rules will be cleared during a re-boot of the system.

Audit:

Run the following commands to verify `iptables` is enabled:

```
# systemctl is-enabled iptables
enabled
```

Run the following command to verify `iptables.service` is active and running or exited

```
# systemctl status iptables | grep -E " Active: active \((running|exited)\) "
```

Active: active (exited) since <day date and time>

Remediation:

Run the following command to enable and start `iptables`:

```
# systemctl --now enable iptables
```


CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.3.3 Configure IPv6 iptables

If IPv6 is not enabled on the system, this section can be skipped.

Iptables is used to set up, maintain, and inspect the tables of IPv6 packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains. Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a 'target', which may be a jump to a user-defined chain in the same table.

Note:

- This section broadly assumes starting with an empty iptables firewall ruleset (established by flushing the rules with iptables -F).
- 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.

The following script will implement the firewall rules of this section and open port 22(ssh) from anywhere. This needs to be updated to only allow systems requiring ssh connectivity to connect as per site policy.

```
#!/bin/bash

# Flush iptables rules
iptables -F

# Ensure default deny firewall policy
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# Ensure loopback traffic is configured
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
iptables -A INPUT -s ::1 -j DROP

# Ensure outbound and established connections are configured
iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT

# Open inbound ssh(tcp port 22) connections
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

3.5.3.3.1 Ensure iptables 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 (::1).

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 (::1) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Note: Changing firewall settings while connected over network can result in being locked out of the system.

Audit:

Run the following commands and verify output includes the listed rules in order (packet and byte counts may differ):

```
# iptables -L INPUT -v -n
Chain INPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source
destination
    0     0 ACCEPT      all  --  lo      *       ::/0
    0     0 DROP        all  --  *       *       ::1
                                     ::/0

# iptables -L OUTPUT -v -n
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source
destination
    0     0 ACCEPT      all  --  *       lo      ::/0
                                     ::/0
```

OR verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

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

ipv6_chk()
{
    passing=""
    grubfile="$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o
-name 'grub.cfg' \) \
    -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;)"
    ! grep -P -- "^h*(kernelopts=|linux|kernel)" "$grubfile" | grep -vq --
ipv6.disable=1 && passing="true"
    grep -Pq -- "^s*net\.ipv6\.conf\.all\.disable_ipv6h*=\h*1\h*(#.*)?$" \
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    grep -Pq -- "^h*net\.ipv6\.conf\.default\.disable_ipv6h*=\h*1\h*(#.*)?$"
\
    /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    sysctl net.ipv6.conf.all.disable_ipv6 | \
    grep -Pq -- "^h*net\.ipv6\.conf\.all\.disable_ipv6h*=\h*1\h*(#.*)?$" &&
\
    sysctl net.ipv6.conf.default.disable_ipv6 | \
    grep -Pq -- "^h*net\.ipv6\.conf\.default\.disable_ipv6h*=\h*1\h*(#.*)?$"
&& passing="true"
    if [ "$passing" = true ] ; then
        echo -e "\nIPv6 is disabled on the system\n"
    else
        echo -e "\nIPv6 is enabled on the system\n"
    fi
}
ipv6_chk
```

Remediation:

Run the following commands to implement the loopback rules:

```
# ip6tables -A INPUT -i lo -j ACCEPT
# ip6tables -A OUTPUT -o lo -j ACCEPT
# ip6tables -A INPUT -s ::1 -j DROP
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.3.3.2 Ensure iptables outbound and established connections are configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Configure the firewall rules for new outbound, and established IPv6 connections.

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

Note: Changing firewall settings while connected over network can result in being locked out of the system.

Audit:

Run the following command and verify all rules for new outbound, and established connections match site policy:

```
# iptables -L -v -n
```

OR verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

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

ipv6_chk()
{
    passing=""
    grubfile="$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o
-name 'grub.cfg' \) \
    -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;)"
    ! grep -P -- "^h*(kernelopts=|linux|kernel)" "$grubfile" | grep -vq --
ipv6.disable=1 && passing="true"
    grep -Pq -- "^s*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*?)?$" \
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    grep -Pq -- "^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*?)?$"
\
    /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    sysctl net.ipv6.conf.all.disable_ipv6 | \
    grep -Pq -- "^h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*?)?$" &&
\
    sysctl net.ipv6.conf.default.disable_ipv6 | \
    grep -Pq -- "^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*?)?$"
&& passing="true"
    if [ "$passing" = true ] ; then
        echo -e "\nIPv6 is disabled on the system\n"
    else
        echo -e "\nIPv6 is enabled on the system\n"
    fi
}
ipv6_chk
```

Remediation:

Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

```
# iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
# iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
# iptables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.3.3.3 Ensure iptables firewall rules exist for all open ports (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

Rationale:

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

Note:

- Changing firewall settings while connected over network can result in being locked out of the system.
- The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy.

Audit:

Run the following command to determine open ports:

# ss -6tuln						
Netid	State	Recv-Q	Send-Q	Local	Address:Port	Peer
Address:Port						
udp	UNCONN	0	0		:::1:123	
:::*						
udp	UNCONN	0	0		:::123	
:::*						
tcp	LISTEN	0	128		:::22	
:::*						
tcp	LISTEN	0	20		:::1:25	
:::*						

Run the following command to determine firewall rules:

```
# iptables -L INPUT -v -n

Chain INPUT (policy DROP 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source
destination
    0     0 ACCEPT     all  --  lo     *       ::/0           ::/0
    0     0 DROP       all  --  *      *       ::1            ::/0
    0     0 ACCEPT     tcp  --  *      *       ::/0           ::/0
tcp dpt:22 state NEW
```

Verify all open ports listening on non-localhost addresses have at least one firewall rule.
The last line identified by the "tcp dpt:22 state NEW" identifies it as a firewall rule for new connections on tcp port 22.

OR verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

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

ipv6_chk()
{
    passing=""
    grubfile="$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o
-name 'grub.cfg' \) \
    -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;)"
    ! grep -P -- "^h*(kernelopts=|linux|kernel)" "$grubfile" | grep -vq --
ipv6.disable=1 && passing="true"
    grep -Pq -- "\s*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#\.*)?$" \
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    grep -Pq -- "^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#\.*)?$"
\
    /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    sysctl net.ipv6.conf.all.disable_ipv6 | \
    grep -Pq -- "^h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#\.*)?$" &&
\
    sysctl net.ipv6.conf.default.disable_ipv6 | \
    grep -Pq -- "^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#\.*)?$"
&& passing="true"
    if [ "$passing" = true ] ; then
        echo -e "\nIPv6 is disabled on the system\n"
    else
        echo -e "\nIPv6 is enabled on the system\n"
    fi
}

ipv6_chk
```

Remediation:

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:

```
# iptables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j ACCEPT
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers 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 Apply Host-based Firewalls or Port Filtering 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.			

3.5.3.3.4 Ensure iptables default deny firewall policy (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.

Rationale:

With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Note: Changing firewall settings while connected over network can result in being locked out of the system.

Audit:

Run the following command and verify that the policy for the INPUT, OUTPUT, and FORWARD chains is DROP or REJECT:

```
# iptables -L
Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy DROP)
```

OR

Verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

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

ipv6_chk()
{
    passing=""
    grubfile="$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o
-name 'grub.cfg' \) \
    -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;)"
    ! grep -P -- "^h*(kernelopts=|linux|kernel)" "$grubfile" | grep -vq --
ipv6.disable=1 && passing="true"
    grep -Pq -- "^s*net\.ipv6\.conf\.all\.disable_ipv6h*=\h*1\h*(#.*?)?$" \
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    grep -Pq -- "^h*net\.ipv6\.conf\.default\.disable_ipv6h*=\h*1\h*(#.*?)?$"
\
    /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    sysctl net.ipv6.conf.all.disable_ipv6 | \
    grep -Pq -- "^h*net\.ipv6\.conf\.all\.disable_ipv6h*=\h*1\h*(#.*?)?$" &&
\
    sysctl net.ipv6.conf.default.disable_ipv6 | \
    grep -Pq -- "^h*net\.ipv6\.conf\.default\.disable_ipv6h*=\h*1\h*(#.*?)?$"
&& passing="true"
    if [ "$passing" = true ] ; then
        echo -e "\nIPv6 is disabled on the system\n"
    else
        echo -e "\nIPv6 is enabled on the system\n"
    fi
}
ipv6_chk
```

Remediation:

Run the following commands to implement a default DROP policy:

```
# ip6tables -P INPUT DROP
# ip6tables -P OUTPUT DROP
# ip6tables -P FORWARD DROP
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.3.3.5 Ensure iptables rules are saved (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `iptables-services` package includes the `/etc/sysconfig/iptables` file. The `iptables` rules in this file will be loaded by the `iptables.service` during boot, or when it is started or re-loaded.

Rationale:

If the `iptables` rules are not saved and a system re-boot occurs, the `iptables` rules will be lost.

Audit:

Review the file `/etc/sysconfig/iptables` and ensure it contains the complete correct rule-set.

Example: `/etc/sysconfig/iptables`

```
# sample configuration for iptables service
# you can edit this manually or use system-config-firewall
# Generated by iptables-save v1.4.21 on Wed Mar 25 14:23:37 2020
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -s ::1/128 -j DROP
-A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Wed Mar 25 14:58:32 2020
```

OR

Verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

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

ipv6_chk()
{
    passing=""
    grubfile="$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o
-name 'grub.cfg' \) \
    -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;)"
    ! grep -P -- "^h*(kernelopts=|linux|kernel)" "$grubfile" | grep -vq --
ipv6.disable=1 && passing="true"
    grep -Pq -- "^s*net\.ipv6\.conf\.all\.disable_ipv6h*=\h*1\h*(#.*?)?$" \
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    grep -Pq -- "^h*net\.ipv6\.conf\.default\.disable_ipv6h*=\h*1\h*(#.*?)?$"
\
    /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    sysctl net.ipv6.conf.all.disable_ipv6 | \
    grep -Pq -- "^h*net\.ipv6\.conf\.all\.disable_ipv6h*=\h*1\h*(#.*?)?$" &&
\
    sysctl net.ipv6.conf.default.disable_ipv6 | \
    grep -Pq -- "^h*net\.ipv6\.conf\.default\.disable_ipv6h*=\h*1\h*(#.*?)?$"
&& passing="true"
    if [ "$passing" = true ] ; then
        echo -e "\nIPv6 is disabled on the system\n"
    else
        echo -e "\nIPv6 is enabled on the system\n"
    fi
}
ipv6_chk
```


Remediation:

Run the following commands to create or update the `/etc/sysconfig/ip6tables` file:

Run the following command to review the current running `iptables` configuration:

```
# ip6tables -L
```

Output should include:

```
Chain INPUT (policy DROP)
target     prot opt source                destination
ACCEPT     all  --  anywhere              anywhere
DROP       all  --  localhost            anywhere
ACCEPT     tcp  --  anywhere              anywhere    state
ESTABLISHED
ACCEPT     udp  --  anywhere              anywhere    state
ESTABLISHED
ACCEPT     icmp --  anywhere              anywhere    state
ESTABLISHED
ACCEPT     tcp  --  anywhere              anywhere    tcp dpt:ssh
state NEW

Chain FORWARD (policy DROP)
target     prot opt source                destination

Chain OUTPUT (policy DROP)
target     prot opt source                destination
ACCEPT     all  --  anywhere              anywhere
ACCEPT     tcp  --  anywhere              anywhere    state
NEW,ESTABLISHED
ACCEPT     udp  --  anywhere              anywhere    state
NEW,ESTABLISHED
ACCEPT     icmp --  anywhere              anywhere    state
NEW,ESTABLISHED
```

Run the following command to save the verified running configuration to the file

`/etc/sysconfig/ip6tables`:

```
# service ip6tables save
ip6tables: Saving firewall rules to /etc/sysconfig/ip6table[ OK ]
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.3.3.6 Ensure ip6tables is enabled and running (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`ip6tables.service` is a utility for configuring and maintaining `ip6tables`.

Rationale:

`ip6tables.service` will load the `iptables` rules saved in the file `/etc/sysconfig/ip6tables` at boot, otherwise the `ip6tables` rules will be cleared during a re-boot of the system.

Audit:

Run the following commands to verify `ip6tables` is enabled:

```
# systemctl is-enabled ip6tables
enabled
```

Run the following command to verify `ip6tables.service` is active and running or exited

```
# systemctl status ip6tables | grep -E " Active: active \((running|exited)\)"
Active: active (exited) since <day date and time>
```

OR verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

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

ipv6_chk()
{
    passing=""
    grubfile="$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o
-name 'grub.cfg' \) \
    -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;)"
    ! grep -P -- "^h*(kernelopts=|linux|kernel)" "$grubfile" | grep -vq --
ipv6.disable=1 && passing="true"
    grep -Pq -- "^s*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*?)?$" \
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    grep -Pq -- "^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*?)?$"
\
    /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    sysctl net.ipv6.conf.all.disable_ipv6 | \
    grep -Pq -- "^h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*?)?$" &&
\
    sysctl net.ipv6.conf.default.disable_ipv6 | \
    grep -Pq -- "^h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*?)?$"
&& passing="true"
    if [ "$passing" = true ] ; then
        echo -e "\nIPv6 is disabled on the system\n"
    else
        echo -e "\nIPv6 is enabled on the system\n"
    fi
}
ipv6_chk
```

Remediation:

Run the following command to enable and start `ip6tables`:

```
# systemctl --now start ip6tables
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> 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> 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.			

3.5.4 Ensure IP tunnels are not configured (Automated)

Profile Applicability:

- STIG

Description:

The operating system must not have unauthorized IP tunnels configured.

Rationale:

IP tunneling mechanisms can be used to bypass network filtering. If tunneling is required, it must be documented with the the Authorizing Official of the organization.

Audit:

Verify the system does not have unauthorized IP tunnels configured.

Check to see if `libreswan` is installed with the following command:

```
# yum list installed libreswan
libreswan.x86_64 3.20-5.el7_4
```

If `libreswan` is installed, check to see if the `IPsec` service is active with the following command:

```
# systemctl status ipsec
ipsec.service - Internet Key Exchange (IKE) Protocol Daemon for IPsec
Loaded: loaded (/usr/lib/systemd/system/ipsec.service; disabled)
Active: inactive (dead)
```

If the `IPsec` service is active, check to see if any tunnels are configured in `/etc/ipsec.conf` and `/etc/ipsec.d/` with the following commands:

```
# grep -iw conn /etc/ipsec.conf /etc/ipsec.d/*.conf
```

If there are indications that a `conn` parameter is configured for a tunnel, ask if the tunnel is documented.

If `libreswan` is installed, `IPsec` is active, and an undocumented tunnel is active, refer to the remediation procedure below.

Remediation:

Remove all unapproved tunnels from the system, or document them with the Authorizing Official.

To remove them edit the `/etc/ipsec.conf` and `/etc/ipsec.d/*.conf` files removing any lines indicating a `conn` parameter is configured.

Example: `vim /etc/ipsec.conf`

Remove and lines with a "conn" parameter set.

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204629
Rule ID: SV-204629r603261_rule
STIG ID: RHEL-07-040820
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> 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> 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 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. See the `ntpd(8)` manual page for more information on configuring NTP.

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`).

4.1 Configure System Accounting (auditd)

System auditing, through `auditd`, allows system administrators to monitor their systems such that they can detect unauthorized access or modification of data. By default, `auditd` will audit system logins, account modifications, and authentication events. Events will be logged to `/var/log/audit/audit.log`. The recording of these events will use a modest amount of disk space on a system. If significantly more events are captured, additional on system or off system storage may need to be allocated.

Note:

- *The recommendations in this section implement an audit policy that produces large quantities of logged data. In some environments it can be challenging to store or process these logs and as such they are marked as Level 2 for both Servers and Workstations.*
- *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. For 32 bit systems, only one rule is needed.*
- *Several recommendations in this section filter based off of `auditd>=500` for unprivileged non-system users. Some systems may have a non-default `UID_MIN` setting, consult the `UID_MIN` setting in `/etc/login.defs` to determine the `UID_MIN` setting for your system.*
- *Once all audit rules have been added to a file or files in the `/etc/audit/rules.d/` directory, **the auditd service must be re-started, or the system rebooted, for the new rules to be included.***
- *The audit and remediation in this section look for a 'key' value. **The 'key' value may be different for the audit settings on your system.***

4.1.1 Ensure auditing is enabled

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

4.1.1.1 Ensure auditd is installed (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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.

Audit:

Run the following command and verify auditd is installed:

```
# rpm -q audit audit-libs  
audit-<version>  
audit-libs-<version>
```

Remediation:

Run the following command to install auditd

```
# yum install audit audit-libs
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

4.1.1.2 Ensure auditd service is enabled and running (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
enabled
```

Run the following command to verify that `auditd` is active:

```
# systemctl is-active auditd.service
active
```

Remediation:

Run the following command to enable and start `auditd`:

```
# systemctl --now enable auditd
```

References:

1. CCI: CCI-000126: The organization determines that the organization-defined subset of the auditable events defined in AU-2 are to be audited within the information system.
2. NIST SP 800-53 :: AU-2 d
3. NIST SP 800-53A :: AU-2.1 (v)
4. NIST SP 800-53 Revision 4 :: AU-2 d
5. CCI-000131: The information system generates audit records containing information that establishes when an event occurred.
6. NIST SP 800-53 :: AU-3
7. NIST SP 800-53A :: AU-3.1
8. NIST SP 800-53 Revision 4 :: AU-3

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204503
Rule ID: SV-204503r603261_rule
STIG ID: RHEL-07-030000
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

4.1.1.3 Ensure auditing for processes that start prior to auditd is enabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Configure `grub` 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.

Note: This recommendation is designed around the `grub2` bootloader, if `LILLO` or another bootloader is in use in your environment enact equivalent settings.

Audit:

Run the following command to verify that the `audit=1` parameter is set:

```
# grep -P -- '^h*(kernelopts=|linux|kernel)' $(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg' \) -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;) | grep -Ev -- '(audit=1\b)'
```

Nothing should be returned

Remediation:

Edit `/etc/default/grub` and add `audit=1` to `GRUB_CMDLINE_LINUX`:

```
GRUB_CMDLINE_LINUX="audit=1"
```

Run the following script to update the `grub2` configuration:

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

GFCU()
{
    grubfile=$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o -
name 'grub.cfg' \) -exec grep -Pl '^h*(kernelopts=|linux|kernel)' {} \;)
    grubdir=$(dirname "$grubfile")
    grub2-mkconfig -o "$grubdir/grub.cfg"
}

GFCU
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

4.1.2 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.

4.1.2.1 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.

Notes:

- *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.*

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 max_log_file /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>
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> 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> Ensure that all systems that store logs have adequate storage space for the logs generated.			

4.1.2.2 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
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.4 <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.			

4.1.2.3 Ensure audit system is set to single when the disk is full. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that the audit system takes appropriate action when the audit storage volume is full.

Rationale:

Taking appropriate action in case of a filled audit storage volume will minimize the possibility of losing audit records.

Audit:

Verify the action the operating system takes if the disk the audit records are written to becomes full.

To determine the action that takes place if the disk is full on the remote server, is set to `syslog`, `single`, or `halt` using the following command:

```
# grep -i disk_full_action /etc/audit/auditd.conf
disk_full_action = single
```

If the value of the `disk_full_action` option is not `syslog`, `single`, or `halt`, or the line is commented out, refer to the remediation procedure below.

Remediation:

Configure the action the operating system takes if the disk the audit records are written to becomes full.

Uncomment or edit the `disk_full_action` option in `/etc/audit/auditd.conf`.

Example: `vim /etc/audit/auditd.conf`

Set it to `syslog`, `single`, or `halt`, such as the following example:

```
disk_full_action = single
```

References:

1. CCI: CCI-001851: The information system off-loads audit records per organization-defined frequency onto a different system or media than the system being audited.
2. NIST SP 800-53 Revision 4 :: AU-4 (1)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204511
Rule ID: SV-204511r603261_rule
STIG ID: RHEL-07-030320
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.2.4 Ensure system notification is sent out when volume is 75% full (Manual)

Profile Applicability:

- STIG

Description:

The operating system must initiate an action to notify the Authorizing Official, at a minimum, when allocated audit record storage volume reaches 75% 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 initiates 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.

Check the system configuration to determine the partition the audit records are being written to 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 that audit records are written to (with the example being /var/log/audit/):

```
# df -h /var/log/audit/  
0.9G /var/log/audit
```

If the audit records are not being written to a partition specifically created for audit records (in this example /var/log/audit is a separate partition), determine the amount of space other files in the partition are currently occupying with the following command:

```
# du -sh <partition>  
1.8G /var
```

Determine what the threshold is for the system to take action when 75 percent of the repository maximum audit record storage capacity is reached:

```
# grep -iw space_left /etc/audit/auditd.conf  
space_left = 225
```

If the value of the `space_left` keyword is not set to 75 percent of the total partition size, refer to the remediation procedure below.

Remediation:

Configure the operating system to initiate an action to notify the Authorizing Official (at a minimum) when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity.

Check the system configuration to determine the partition the audit records are being written to:

```
# grep -iw log_file /etc/audit/auditd.conf
```

Determine the size of the partition that audit records are written to (with the example being `/var/log/audit/`):

```
# df -h /var/log/audit/
```

Set the value of the `space_left` keyword in `/etc/audit/auditd.conf` to 75 percent of the partition size.

Example: `vim /etc/audit/auditd.conf`

Add the line with `space_left` set to 75% or the partition size.

Example:

```
space_left = 225
```

References:

1. CCI-001855: The information system provides a warning to organization-defined personnel, roles, and/or locations within organization-defined time period when allocated audit record storage volume reaches organization-defined percentage of repository maximum audit record storage capacity.
2. NIST SP 800-53 Revision 4 :: AU-5 (1)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204513
Rule ID: SV-204513r744112_rule
STIG ID: RHEL-07-030330
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.2.5 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 when the audit logs are full.

Rationale:

In high security contexts, the risk of detecting unauthorized access or nonrepudiation exceeds the benefit of the system's availability.

Audit:

Run the following commands and verify output matches:

```
# grep space_left_action /etc/audit/auditd.conf

space_left_action = email
# grep action_mail_acct /etc/audit/auditd.conf

action_mail_acct = root
# grep admin_space_left_action /etc/audit/auditd.conf

admin_space_left_action = halt
```

Remediation:

Set the following parameters in `/etc/audit/auditd.conf`:

```
space_left_action = email
action_mail_acct = root
admin_space_left_action = halt
```

References:

1. CCI: CCI-001855: The information system provides a warning to organization-defined personnel, roles, and/or locations within organization-defined time period when allocated audit record storage volume reaches organization-defined percentage of repository maximum audit record storage capacity.
2. NIST SP 800-53 Revision 4 :: AU-5 (1)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204514
Rule ID: SV-204514r603261_rule
STIG ID: RHEL-07-030340
Severity: CAT II

Vul ID: V-204515
Rule ID: SV-204515r603261_rule
STIG ID: RHEL-07-030350
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.4 <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.			

4.1.2.6 Ensure audit system action is defined for sending errors (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that the audit system takes appropriate action when there is an error sending audit records to a remote system.

Rationale:

Taking appropriate action when there is an error sending audit records to a remote system will minimize the possibility of losing audit records.

Audit:

Verify the action the operating system takes if there is an error sending audit records to a remote system.

Check the action that takes place if there is an error sending audit records to a remote system is set to `syslog`, `single`, or `halt` with the following command:

```
# grep -i network_failure_action /etc/audit/auditd.conf
network_failure_action = syslog
```

If the value of the `network_failure_action` option is not `syslog`, `single`, or `halt`, or the line is commented out, refer to the remediation below.

Remediation:

Configure the action the operating system takes if there is an error sending audit records to a remote system.

Uncomment the `network_failure_action` option in `/etc/audit/auditd.conf` and set it to `syslog`, `single`, or `halt`.

Example: `vim /etc/audit/auditd.conf`

Add the line as shown in below

```
network_failure_action = syslog
```

References:

1. CCI: CCI-001851: The information system off-loads audit records per organization-defined frequency onto a different system or media than the system being audited.
2. NIST SP 800-53 Revision 4 :: AU-4 (1)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204512
Rule ID: SV-204512r603261_rule
STIG ID: RHEL-07-030321
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.2.7 Ensure audit_backlog_limit is sufficient (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

The backlog limit has a default setting of 64

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:

Run the following command to verify the audit_backlog_limit= parameter is set to an appropriate size for your organization

```
# grep -Ph -- '^h*(kernelopts=|linux|kernel)' $(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg' \) -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;) | grep -Pom1 -- '(audit_backlog_limit=\d+\b)'
```

Example output:

```
audit_backlog_limit=8192
```

Ensure the returned value complies with local site policy. It's recommended that this value be 8192 or larger.

Remediation:

Edit /etc/default/grub and add `audit_backlog_limit=<BACKLOG SIZE>` to

GRUB_CMDLINE_LINUX:

Example:

```
GRUB_CMDLINE_LINUX="audit_backlog_limit=8192"
```

Run the following script to update the grub2 configuration:

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

GFCU()
{
    grubfile=$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o -
name 'grub.cfg' \) -exec grep -Pl '^h*(kernelopts=|linux|kernel)' {} \;)
    grubdir=$(dirname "$grubfile")
    grub2-mkconfig -o "$grubdir/grub.cfg"
}
GFCU
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

4.1.2.8 Ensure audit logs are stored on a different system. (Manual)

Profile Applicability:

- STIG

Description:

The operating system must off-load audit records 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.

Audit:

Verify the operating system off-loads audit records onto a different system or media from the system being audited.

To determine the remote server that the records are being sent to, use the following command:

```
# grep -i remote_server /etc/audit/auditd.conf
remote_server = 10.0.21.1
```

If a remote server is not configured, or the line is commented out, ask 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, refer to the remediation procedure below.

Remediation:

Configure the operating system to off-load audit records onto a different system or media from the system being audited.

Set the remote server option in `/etc/audit/auditd.conf` with the IP address of the log aggregation server.

Example: `vim /etc/audit/auditd.conf`

Add, uncomment or update the following line:

Note: The ip address listed is just for an example. Replace it with the IP address or the log aggregation server in your environment.

```
remote_server = 10.0.21.1
```

References:

1. CCI: CCI-001851: The information system off-loads audit records per organization-defined frequency onto a different system or media than the system being audited.
2. NIST SP 800-53 Revision 4 :: AU-4 (1)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204509
Rule ID: SV-204509r603261_rule
STIG ID: RHEL-07-030300
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.2.9 Ensure audit logs on separate system are encrypted. (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 and encrypted the records.

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading and encrypting is a common process in information systems with limited audit storage capacity.

Audit:

Verify the operating system encrypts audit records off-loaded onto a different system or media from the system being audited.

To determine if the transfer is encrypted, use the following command:

```
# grep -i enable_krb5 /etc/audit/auditd.conf
enable_krb5 = yes
```

If the value of the `enable_krb5` option is not set to `yes` or the line is commented out, ask 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, refer to the remediation procedure below.

Remediation:

Configure the operating system to encrypt the transfer of off-loaded audit records onto a different system or media from the system being audited.

Add or update the `/etc/audit/auditd.conf` and set it with the following line:

Example: `vim /etc/audit/auditd.conf`

Add, uncomment or update the following line:

```
enable_krb5 = yes
```

References:

1. CCI: CCI-001851: The information system off-loads audit records per organization-defined frequency onto a different system or media than the system being audited.
2. NIST SP 800-53 Revision 4 :: AU-4 (1)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204510
Rule ID: SV-204510r603261_rule
STIG ID: RHEL-07-030310
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8 <u>Audit Log Management</u> Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.2.10 Ensure the auditing processing failures are handled. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must shut down upon audit processing failure, unless availability is an overriding concern. If availability is a concern, the system must alert the designated staff in the event 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.

Impact:

Kernel log monitoring must also be configured to properly alert designated staff.

Audit:

Confirm the audit configuration regarding how auditing processing failures are handled. Check to see what level `auditctl` is set to with following command:

```
# auditctl -s | grep -i "fail"
failure 2
```

If the value of `failure` is set to 2, the system is configured to panic (shut down) in the event of an auditing failure.

If the value of `failure` is set to 1, the system is configured to only send information to the kernel log regarding the failure.

If the `failure` setting is not set, this is a CAT I finding, refer to the remediation procedure below.

If the `failure` setting is set to any value other than 1 or 2, this is a CAT II finding, refer to the remediation procedure below.

If the `failure` setting is set to 1 but the availability concern is not documented or there is no monitoring of the kernel log, this is a CAT III finding, refer to the remediation procedure below.

Remediation:

Configure the operating system to shut down or notify staff in the event of an audit processing failure.

To add or correct the option to shut down the operating system use the following command:

```
# auditctl -f 2
```

Edit the `/etc/audit/rules.d/audit.rules` file and add the following line:

Example: `vim /etc/audit/rules.d/audit.rules`

Add this line:

```
-f 2
```

If availability has been determined to be more important, and this decision is documented with the Authorizing Official, configure the operating system to notify the appropriate staff in the event of an audit processing failure with the following command:

```
# auditctl -f 1
```

Edit the `/etc/audit/rules.d/audit.rules` file and add the following line:

Example: `vim /etc/audit/rules.d/audit.rules`

Add this line:

```
-f 1
```

The audit daemon must be restarted for changes to take effect:

```
# service auditd restart
```

References:

1. CCI: CCI-000139: The information system alerts designated organization-defined personnel or roles in the event of an audit processing failure.
2. NIST SP 800-53 :: AU-5 a
3. NIST SP 800-53A :: AU-5.1 (ii)
4. NIST SP 800-53 Revision 4 :: AU-5 a

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204504
Rule ID: SV-204504r603261_rule
STIG ID: RHEL-07-030010
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.2.11 Ensure off-load of audit logs. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must configure the au-remote plugin to off-load audit logs using the audisp-remote daemon.

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.

Without the configuration of the "au-remote" plugin, the audisp-remote daemon will not off load the logs from the system being audited.

Audit:

Verify the `au-remote` plugin is configured to always off-load audit logs using the audisp-remote daemon:

```
# cat /etc/audisp/plugins.d/au-remote.conf | grep -v "^#"
active = yes
direction = out
path = /sbin/audisp-remote
type = always
format = string
```

If the `direction` setting is not set to `out`, or the line is commented out, refer to the remediation procedure below.

If the `path` setting is not set to `/sbin/audisp-remote`, or the line is commented out, refer to the remediation procedure below.

If the `type` setting is not set to `always`, or the line is commented out, refer to the remediation procedure below.

Remediation:

Edit the `/etc/audit/plugins.d/au-remote.conf` file and add, uncomment or update the following values:

Example: `vim /etc/audit/plugins.d/au-remote.conf`

Add uncomment or update the following lines:

```
direction = out
path = /sbin/auditd-remote
type = always
```

The audit daemon must be restarted for changes to take effect:

```
# service auditd restart
```

References:

1. CCI: CCI-001851: The information system off-loads audit records per organization-defined frequency onto a different system or media than the system being audited.
2. NIST SP 800-53 Revision 4 :: AU-4 (1)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204506
Rule ID: SV-204506r603261_rule
STIG ID: RHEL-07-030201
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.2.12 Ensure action is taken when audisp-remote buffer is full (Automated)

Profile Applicability:

- STIG

Description:

The operating system must take appropriate action when the audisp-remote buffer 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.

When the remote buffer is full, audit logs will not be collected and sent to the central log server.

Audit:

Verify the audisp daemon is configured to take an appropriate action when the internal queue (audisp-remote buffer) is full:

```
# grep "overflow_action" /etc/audisp/audispd.conf
overflow_action = syslog
```

If the `overflow_action` option is not `syslog`, `single`, or `halt`, or the line is commented out, refer to the remediation procedure below.

Remediation:

Edit the `/etc/audisp/audispd.conf` file and add or update the `overflow_action` option:

Example: `vim /etc/audisp/audispd.conf`

Add, update or uncomment the following line:

```
overflow_action = syslog
```

The audit daemon must be restarted for changes to take effect:

```
# service auditd restart
```

References:

1. CCI: CCI-001851: The information system off-loads audit records per organization-defined frequency onto a different system or media than the system being audited.
2. NIST SP 800-53 Revision 4 :: AU-4 (1)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204507
Rule ID: SV-204507r603261_rule
STIG ID: RHEL-07-030210
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.2.13 Ensure off-loaded audit logs are labeled. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must label all off-loaded audit logs before sending them to the central log server.

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.

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 audisp daemon is configured to label all off-loaded audit logs by checking that the `name_format` `hostname`, `fqd`, or `numeric`:

```
# grep "name_format" /etc/audisp/audispd.conf  
name_format = hostname
```

If the `name_format` option is not `hostname`, `fqd`, or `numeric`, or the line is commented out, refer to the remediation procedure below.

Remediation:

Edit the `/etc/audit/auditd.conf` file and add or update the `name_format` option:

Example: `vim /etc/audit/auditd.conf`

Add the name format to include `hostname`, `fqdn`, or `numeric`.

Example:

```
name_format = hostname
```

The audit daemon must be restarted for changes to take effect:

```
# service auditd restart
```

References:

1. CCI: CCI-001851: The information system off-loads audit records per organization-defined frequency onto a different system or media than the system being audited.
2. NIST SP 800-53 Revision 4 :: AU-4 (1)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204508
Rule ID: SV-204508r603261_rule
STIG ID: RHEL-07-030211
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3 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/audit.d/` directory.

4.1.3.1 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) or `clock_settime` (allows for the setting of several internal clocks and timers) system calls have been executed and always write an audit record to the `/var/log/audit.log` file upon exit, tagging the records with the identifier "time-change"

Note: Reloading the auditd config to set active settings requires the `auditd` service to be restarted, and may require a system reboot.

Rationale:

Unexpected changes in system date and/or time could be a sign of malicious activity on the system.

Audit:

On a 32 bit system run the following commands:

```
# grep time-change /etc/audit/rules.d/*.rules  
# auditctl -l | grep time-change
```

Verify output of both matches:

```
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-  
change  
-a always,exit -F arch=b32 -S clock_settime -k time-change  
-w /etc/localtime -p wa -k time-change
```

On a 64 bit system run the following commands:

```
# grep time-change /etc/audit/rules.d/*.rules  
# auditctl -l | grep time-change
```

Verify output of both matches:

```
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change  
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-  
change  
-a always,exit -F arch=b64 -S clock_settime -k time-change  
-a always,exit -F arch=b32 -S clock_settime -k time-change  
-w /etc/localtime -p wa -k time-change
```

Remediation:

For 32 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

Example: vi /etc/audit/rules.d/50-time_change.rules

Add the following lines:

```
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
```

For 64 bit systems Edit or create a file in the /etc/audit/rules.d/ directory ending in .rules

Example: vi /etc/audit/rules.d/50-time_change.rules

Add the following lines:

```
-a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change
-a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change
-a always,exit -F arch=b64 -S clock_settime -k time-change
-a always,exit -F arch=b32 -S clock_settime -k time-change
-w /etc/localtime -p wa -k time-change
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs 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	5.5 Implement Automated Configuration Monitoring Systems 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.			

4.1.3.2 Ensure system administrator command executions (sudo) are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

`sudo` provides users with temporary elevated privileges to perform operations. Monitor the administrator with temporary elevated privileges and the operation(s) they performed.

Rationale:

creating an audit log of administrators 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 logfile` to verify if unauthorized commands have been executed.

Note: Systems may have been customized to change the default `UID_MIN`. To confirm the `UID_MIN` for your system, run the following command:

```
# awk '/^\s*UID_MIN/{print $2}' /etc/login.defs
```

If your systems' `UID_MIN` is not `1000`, replace `audit>=1000` with `audit>=<UID_MIN for your system>` in the Audit and Remediation procedures.

Reloading the `auditd` config to set active settings may require a system reboot.

Audit:

On a 32 bit system run the following commands:

Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep actions /etc/audit/rules.d/*.rules
```

Verify the output includes:

```
/etc/audit/rules.d/cis.rules:-a exit,always -F arch=b32 -C euid!=uid -F euid=0 -F auid>=1000 -F auid!=4294967295 -S execve -k actions
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep actions
```

Verify the output includes:

```
-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -F auid>=1000 -F auid!=-1 -F key=actions
```

On a 64 bit system run the following commands:

Run the following command to verify the rules are contained in a `.rules` file in the `/etc/audit/rules.d/` directory:

```
# grep actions /etc/audit/rules.d/*.rules
```

Verify the output includes:

```
-a exit,always -F arch=b64 -C euid!=uid -F euid=0 -F auid>=1000 -F auid!=4294967295 -S execve -k actions  
-a exit,always -F arch=b32 -C euid!=uid -F euid=0 -F auid>=1000 -F auid!=4294967295 -S execve -k actions
```

Run the following command to verify that rules are in the running `auditd` config:

```
# auditctl -l | grep actions
```

Verify the output includes:

```
-a always,exit -F arch=b64 -S execve -C uid!=euid -F euid=0 -F auid>=1000 -F auid!=-1 -F key=actions  
-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -F auid>=1000 -F auid!=-1 -F key=actions
```

Remediation:

For 32 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`:

Example: `vi /etc/audit/rules.d/50-actions.rules`

Add the following line:

```
-a exit,always -F arch=b32 -C euid!=uid -F euid=0 -F auid>=1000 -F
auid!=4294967295 -S execve -k actions
```

For 64 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`:

Example: `vi /etc/audit/rules.d/50-actions.rules`

Add the following lines:

```
-a always,exit -F arch=b64 -C euid!=uid -F euid=0 -F auid>=1000 -F
auid!=4294967295 -S execve -k actions
-a always,exit -F arch=b32 -C euid!=uid -F euid=0 -F auid>=1000 -F
auid!=4294967295 -S execve -k actions
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	4.9 <u>Log and Alert on Unsuccessful Administrative Account Login</u> Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.			

4.1.3.3 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. The file `/var/run/utmp` tracks all currently logged in users. All audit records will be tagged with the identifier "session." The `/var/log/wtmp` file tracks logins, logouts, shutdown, and reboot events. The file `/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 "logins."

Notes:

- *The `last` command can be used to read `/var/log/wtmp` (`last` with no parameters) and `/var/run/utmp` (`last -f /var/run/utmp`)*
- *Reloading the `auditd` config to set active settings requires the `auditd` service to be restarted, and may require a system reboot.*

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:

Run the following command to check the auditd `.rules` files:

```
# grep -E '(session|logins)' /etc/audit/rules.d/*.rules
```

Verify output includes:

```
-w /var/run/utmp -p wa -k session  
-w /var/log/wtmp -p wa -k logins  
-w /var/log/btmp -p wa -k logins
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep -E '(session|logins)'
```

Verify output includes:

```
-w /var/run/utmp -p wa -k session  
-w /var/log/wtmp -p wa -k logins  
-w /var/log/btmp -p wa -k logins
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`

Example: `vi /etc/audit/rules.d/50-session.rules`

Add the following lines:

```
-w /var/run/utmp -p wa -k session  
-w /var/log/wtmp -p wa -k logins  
-w /var/log/btmp -p wa -k logins
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	4.9 <u>Log and Alert on Unsuccessful Administrative Account Login</u> Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.		●	●
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●
v7	16.13 <u>Alert on Account Login Behavior Deviation</u> Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.1.3.4 Ensure events that modify the system's Mandatory Access Controls are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

Monitor SELinux 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.*
- *Reloading the auditd config to set active settings requires the `auditd` service to be restarted, and may require a system reboot.*

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:

Run the following commands:

```
# grep MAC-policy /etc/audit/rules.d/*.rules
# auditctl -l | grep MAC-policy
```

Verify output of both 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`

Example: `vi /etc/audit/rules.d/50-MAC_policy.rules`

Add the following lines:

```
-w /etc/selinux/ -p wa -k MAC-policy
-w /usr/share/selinux/ -p wa -k MAC-policy
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	5.5 <u>Implement Automated Configuration Monitoring Systems</u> 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.			

4.1.3.5 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 monitor the `sethostname` (set the systems host name) or `setdomainname` (set the systems domainname) system calls, and write an audit event on system call exit. The other parameters monitor the `/etc/issue` and `/etc/issue.net` files (messages displayed pre-login), `/etc/hosts` (file containing host names and associated IP addresses) and `/etc/sysconfig/network` (directory containing network interface scripts and configurations) files.

Note: Reloading the auditd config to set active settings requires the `auditd` service to be restarted, and may require a system reboot.

Rationale:

Monitoring `sethostname` and `setdomainname` will identify potential unauthorized changes to host and domainname 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 in the file 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 will be tagged with the identifier "system-locale."

Audit:

On a 32 bit system run the following commands:

```
# grep system-locale /etc/audit/rules.d/*.rules  
# auditctl -l | grep system-locale
```

Verify output of both matches:

```
-a always,exit -F arch=b32 -S sethostname -S 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/sysconfig/network -p wa -k system-locale
```

On a 64 bit system run the following commands:

```
# grep system-locale /etc/audit/rules.d/*.rules  
# auditctl -l | grep system-locale
```

Verify output of both matches:

```
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale  
-a always,exit -F arch=b32 -S sethostname -S 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/sysconfig/network -p wa -k system-locale
```

Remediation:

For 32 bit systems edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`

Example: `vi /etc/audit/rules.d/50-system_local.rules`

Add the following lines:

```
-a always,exit -F arch=b32 -S sethostname -S 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/sysconfig/network -p wa -k system-locale
```

For 64 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`

Example: `vi /etc/audit/rules.d/50-system_local.rules`

Add the following lines:

```
-a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname -S 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/sysconfig/network -p wa -k system-locale
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	5.5 <u>Implement Automated Configuration Monitoring Systems</u> 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.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.6 Ensure successful file system mounts are collected (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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

Note: Systems may have been customized to change the default `UID_MIN`. To confirm the `UID_MIN` for your system, run the following command:

```
# awk '/^\s*UID_MIN/{print $2}' /etc/login.defs
```

If your systems' `UID_MIN` is not `1000`, replace `audit>=1000` with `audit>=<UID_MIN for your system>` in the Audit and Remediation procedures.

Reloading the `auditd` config to set active settings may require a system reboot.

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 a 32 bit system run the following commands:

Run the following command to check the auditd .rules files:

```
# grep mounts /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k  
mounts
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep mounts
```

Verify output matches:

```
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=-1 -k mounts
```

On a 64 bit system run the following commands:

Run the following command to check the auditd .rules files:

```
# grep mounts /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k  
mounts  
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k  
mounts
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep mounts
```

Verify output matches:

```
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=-1 -k mounts  
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=-1 -k mounts
```

Remediation:

For 32 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`

Example: `vi /etc/audit/rules.d/50-mounts.rules`

Add the following lines:

```
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
```

For 64 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`

Example: `vi /etc/audit/rules.d/50-mounts.rules`

Add the following lines:

```
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
```

Additional Information:

This tracks successful and unsuccessful mount commands.

File system mounts do not have to come from external media and this action still does not verify write (e.g. CD ROMS).

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.7 Ensure kernel module loading and unloading is collected (Automated)

Profile Applicability:

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

Description:

Monitor the loading and unloading of kernel modules. The programs `insmod` (install a kernel module), `rmmod` (remove a kernel module), and `modprobe` (a more sophisticated program to load and unload modules, as well as some other features) control loading and unloading of modules. The `init_module` (load a module) and `delete_module` (delete a module) system calls control loading and unloading of modules. Any execution of the loading and unloading module programs and system calls will trigger an audit record with an identifier of "modules".

Note: Reloading the auditd config to set active settings requires the `auditd` service to be restarted, and may require a system reboot.

Rationale:

Monitoring the use of `insmod`, `rmmod` and `modprobe` could provide system administrators with evidence that an unauthorized user loaded or unloaded a kernel module, possibly compromising the security of the system. Monitoring of the `init_module` and `delete_module` system calls would reflect an unauthorized user attempting to use a different program to load and unload modules.

Audit:

On a 32 bit system run the following commands:

Run the following command to check the auditd .rules files:

```
# grep modules /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b32 -S init_module -S delete_module -k modules
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep modules
```

Verify output matches:

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b32 -S init_module,delete_module -F key=modules
```

On a 64 bit system run the following commands:

Run the following command to check the auditd .rules files:

```
# grep modules /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep modules
```

Verify output matches:

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module,delete_module -F key=modules
```

Remediation:

For 32 bit systems edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`

Example: `vi /etc/audit/rules.d/50-modules.rules`

Add the following lines:

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b32 -S init_module -S delete_module -k modules
```

For 64 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`

Example: `vi /etc/audit/rules.d/50-modules.rules`

Add the following lines:

```
-w /sbin/insmod -p x -k modules
-w /sbin/rmmod -p x -k modules
-w /sbin/modprobe -p x -k modules
-a always,exit -F arch=b64 -S init_module -S delete_module -k modules
```

References:

1. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3
2. NIST SP 800-53 :: AU-12 c
3. NIST SP 800-53A :: AU-12.1 (iv)
4. NIST SP 800-53 Revision 4 :: AU-12 c

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204560
Rule ID: SV-204560r603261_rule
STIG ID: RHEL-07-030820
Severity: CAT II

Vul ID: V-204562
Rule ID: SV-204562r603261_rule
STIG ID: RHEL-07-030830
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.8 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 a file in the `/etc/sudoers.d` directory will be written to when the file or its attributes have changed.

Note: Reloading the auditd config to set active settings may require a system reboot.

Rationale:

Changes in the `/etc/sudoers` file, or a file in the `/etc/sudoers.d/` directory can indicate that an unauthorized change has been made to scope of system administrator activity.

Audit:

Run the following command to check the auditd `.rules` files:

```
# grep scope /etc/audit/rules.d/*.rules
```

Verify output of matches:

```
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d/ -p wa -k scope
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep scope
```

Verify 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`

_Example: `vi /etc/audit/rules.d/50-scope.rules`

Add the following lines:

```
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d/ -p wa -k scope
```

References:

1. CCI: CCI-000130: The information system generates audit records containing information that establishes what type of event occurred.
2. NIST SP 800-53 :: AU-3
3. NIST SP 800-53A :: AU-3.1
4. NIST SP 800-53 Revision 4 :: AU-3
5. CCI-000135: The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.
6. NIST SP 800-53 :: AU-3 (1)
7. NIST SP 800-53A :: AU-3 (1).1 (ii)
8. NIST SP 800-53 Revision 4 :: AU-3 (1)
9. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
10. NIST SP 800-53 :: AU-12 c
11. NIST SP 800-53A :: AU-12.1 (iv)
12. NIST SP 800-53 Revision 4 :: AU-12 c
13. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
14. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204549
Rule ID: SV-204549r603261_rule
STIG ID: RHEL-07-030700
Severity: CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.9 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 following system calls and tags them with the identifier "delete":

- `unlink` - remove a file
- `unlinkat` - remove a file attribute
- `rename` - rename a file
- `renameat` - rename a file attribute

Note: Systems may have been customized to change the default `UID_MIN`. To confirm the `UID_MIN` for your system, run the following command:

```
# awk '/^\s*UID_MIN/{print $2}' /etc/login.defs
```

If your systems' `UID_MIN` is not `1000`, replace `audit>=1000` with `audit>=<UID_MIN for your system>` in the Audit and Remediation procedures.

Reloading the `auditd` config to set active settings may require a system reboot.

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 a 32 bit system run the following commands:

Run the following command to check the auditd .rules files:

```
# grep delete /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F  
auid>=1000 -F auid!=4294967295 -k delete
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep delete
```

Verify output matches:

```
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F  
auid>=1000 -F auid!=4294967295 -k delete
```

On a 64 bit system run the following commands:

Run the following command to check the auditd .rules files:

```
# grep delete /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F  
auid>=1000 -F auid!=4294967295 -k delete  
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F  
auid>=1000 -F auid!=4294967295 -k delete
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep delete
```

Verify output matches:

```
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F  
auid>=1000 -F auid!=-1 -k delete  
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F  
auid>=1000 -F auid!=-1 -k delete
```

Remediation:

For 32 bit systems edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`

Example: `vi /etc/audit/rules.d/50-deletion.rules`

Add the following lines:

```
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F
audit>=1000 -F audit!=4294967295 -k delete
```

For 64 bit systems edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`

Example: `vi /etc/audit/rules.d/50-deletion.rules`

Add the following lines:

```
-a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F
audit>=1000 -F audit!=4294967295 -k delete
-a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F
audit>=1000 -F audit!=4294967295 -k delete
```

References:

1. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3
2. NIST SP 800-53 :: AU-12 c
3. NIST SP 800-53A :: AU-12.1 (iv)
4. NIST SP 800-53 Revision 4 :: AU-12 c
5. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events
6. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

At a minimum, configure the audit system to collect file deletion events for all users and root.

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204569
Rule ID: SV-204569r603261_rule
STIG ID: RHEL-07-030880
Severity: CAT II

Vul ID: V-204570
Rule ID: SV-204570r603261_rule
STIG ID: RHEL-07-030890
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.10 Ensure use of privileged commands is collected (Automated)

Profile Applicability:

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

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.

Note: Systems may have been customized to change the default UID_MIN. To confirm the UID_MIN for your system, run the following command:

```
# awk '/^\s*UID_MIN/{print $2}' /etc/login.defs
```

If your systems' UID_MIN is not 1000, replace `audit>=1000` with `audit>=<UID_MIN for your system>` in the Audit and Remediation procedures.

Reloading the auditd config to set active settings may require a system reboot.

Rationale:

Execution of privileged commands by non-privileged users could be an indication of someone trying to gain unauthorized access to the system.

Audit:

Run the following command replacing `<partition>` with a list of partitions where programs can be executed from on your system:

```
# find <partition> -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk '{print "-a always,exit -F path=" $1 " -F perm=x -F auid>=" $(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs) "' -F auid!=4294967295 -k privileged" }'
```

Verify all resulting lines are a `.rules` file in `/etc/audit/rules.d/` and the output of `auditctl -l`.

Note: The `.rules` file output will be `auid!=-1` not `auid!=4294967295`

Remediation:

To remediate this issue, the system administrator will have to execute a find command to locate all the privileged programs and then add an audit line for each one of them.

The audit parameters associated with this are as follows:

- `-F path=" $1 "` - will populate each file name found through the find command and processed by awk.
- `-F perm=x` - will write an audit record if the file is executed.
- `-F audit>=1000` - will write a record if the user executing the command is not a privileged user.
- `-F auid!= 4294967295` - will ignore Daemon events

All audit records should be tagged with the identifier "privileged".

Run the following command replacing with a list of partitions where programs can be executed from on your system:

```
# find <partition> -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk '{print "-a always,exit -F path=" $1 " -F perm=x -F auid>=" $(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs) "' -F auid!=4294967295 -k privileged" }'
```

Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules` and add all resulting lines to the file.

Example:

```
# find / -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk '{print "-a always,exit -F path=" $1 " -F perm=x -F auid>=" $(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs) "' -F auid!=4294967295 -k privileged" }' >> /etc/audit/rules.d/50-privileged.rules
```

References:

1. CCI: CCI-000130: The information system generates audit records containing information that establishes what type of event occurred.
2. NIST SP 800-53 :: AU-3
3. NIST SP 800-53A :: AU-3.1
4. NIST SP 800-53 Revision 4 :: AU-3
5. CCI-000135: The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.
6. NIST SP 800-53 :: AU-3 (1)
7. NIST SP 800-53A :: AU-3 (1).1 (ii)
8. NIST SP 800-53 Revision 4 :: AU-3 (1)
9. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
10. NIST SP 800-53 :: AU-12 c
11. NIST SP 800-53A :: AU-12.1 (iv)
12. NIST SP 800-53 Revision 4 :: AU-12 c
13. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
14. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204548
Rule ID: SV-204548r603261_rule
STIG ID: RHEL-07-030690
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.11 Ensure unsuccessful unauthorized file access attempts are collected (Automated)

Profile Applicability:

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

Description:

Monitor for unsuccessful attempts to access files. The parameters below are associated with system calls that control creation (`creat`), opening (`open` , `openat`) and truncation (`truncate` , `ftruncate`) of files. An audit log record will only be written if the user is a non-privileged user (`auid>=1000`), is not a Daemon event (`auid=4294967295`) and if the system call returned `EACCES` (permission denied to the file) or `EPERM` (some other permanent error associated with the specific system call). All audit records will be tagged with the identifier "access."

Note: Systems may have been customized to change the default `UID_MIN`. To confirm the `UID_MIN` for your system, run the following command:

```
# awk '/^\s*UID_MIN/{print $2}' /etc/login.defs
```

If your systems' `UID_MIN` is not `1000`, replace `audit>=1000` with `audit>=<UID_MIN for your system>` in the Audit and Remediation procedures.

Reloading the `auditd` config to set active settings may require a system reboot.

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 a 32 bit system run the following commands:

Run the following command to check the auditd .rules files:

```
# grep access /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep access
```

Verify output matches:

```
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=-1 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=-1 -k access
```

On a 64 bit system run the following commands:

Run the following command to check the auditd .rules files:

```
# grep access /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep access
```

Verify output matches:


```
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=-1 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=-1 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=-1 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=-1 -k access
```

Remediation:

For 32 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`

Example: `vi /etc/audit/rules.d/50-access.rules`

Add the following lines:

```
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
```

For 64 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`

Example: `vi /etc/audit/rules.d/50-access.rules`

Add the following lines:

```
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S
ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access
```

References:

1. CCI: CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
2. NIST SP 800-53 :: AU-12 c
3. NIST SP 800-53A :: AU-12.1 (iv)
4. NIST SP 800-53 Revision 4 :: AU-12 c
5. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
6. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204530
Rule ID: SV-204530r603261_rule
STIG ID: RHEL-07-030500
Severity: CAT II

Vul ID: V-204531
Rule ID: SV-204531r603261_rule
STIG ID: RHEL-07-030510
Severity: CAT II

Vul ID: V-204532
Rule ID: SV-204532r603261_rule
STIG ID: RHEL-07-030520
Severity: CAT II

Vul ID: V-204533
Rule ID: SV-204533r603261_rule
STIG ID: RHEL-07-030530
Severity: CAT II

Vul ID: V-204534
Rule ID: SV-204534r603261_rule
STIG ID: RHEL-07-030540
Severity: CAT II

Vul ID: V-204535
Rule ID: SV-204535r603261_rule
STIG ID: RHEL-07-030550
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	14.9 <u>Enforce Detail Logging for Access or Changes to Sensitive Data</u> 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).			

4.1.3.12 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 `chmod`, `fchmod` and `fchmodat` system calls affect the permissions associated with a file. The `chown`, `fchown`, `fchownat` and `lchown` system calls affect owner and group attributes on a file. The `setxattr`, `lsetxattr`, `fsetxattr` (set extended file attributes) and `removexattr`, `lremovexattr`, `fremovexattr` (remove extended file attributes) control extended file attributes. In all cases, an audit record will only be written for non-system user ids (`audit >= 1000`) and will ignore Daemon events (`audit = 4294967295`). All audit records will be tagged with the identifier "perm_mod."

Note: Systems may have been customized to change the default `UID_MIN`. To confirm the `UID_MIN` for your system, run the following command:

```
# awk '/^\s*UID_MIN/{print $2}' /etc/login.defs
```

If your systems' `UID_MIN` is not `1000`, replace `audit >= 1000` with `audit >= <UID_MIN for your system>` in the Audit and Remediation procedures.

Reloading the `auditd` config to set active settings may require a system reboot.

Rationale:

Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Audit:

On a 32 bit system run the following commands:

Run the following command to check the `auditd .rules` files:

```
# grep perm_mod /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep perm_mod
```

Verify output matches:

```
-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=b32 -S setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F auid>=1000 -F auid!=-1 -F key=perm_mod
```

On a 64 bit system run the following commands:

Run the following command to check the auditd .rules files:

```
# grep perm_mod /etc/audit/rules.d/*.rules
```

Verify output matches:

```
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod
```

Run the following command to check loaded auditd rules:

```
# auditctl -l | grep auditctl -l | grep perm_mod
```

Verify 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=b32 -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 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:

For 32 bit systems edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`

Example: `vi /etc/audit/rules.d/50-perm_mod.rules`

Add the following lines:

```
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295
-k perm_mod
```

For 64 bit systems Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`

Example: `vi /etc/audit/rules.d/50-perm_mod.rules`

Add the following lines:

```
-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F
auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F
auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295
-k perm_mod
-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S
removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295
-k perm_mod
```

References:

1. CCI: CCI-000126: The organization determines that the organization-defined subset of the auditable events defined in AU-2 are to be audited within the information system.
2. NIST SP 800-53 :: AU-2 d
3. NIST SP 800-53A :: AU-2.1 (v)
4. NIST SP 800-53 Revision 4 :: AU-2 d
5. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
6. NIST SP 800-53 :: AU-12 c
7. NIST SP 800-53A :: AU-12.1 (iv)
8. NIST SP 800-53 Revision 4 :: AU-12 c

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204517
Rule ID: SV-204517r603261_rule
STIG ID: RHEL-07-030370
Severity: CAT II

Vul ID: V-204518
Rule ID: SV-204518r603261_rule
STIG ID: RHEL-07-030380
Severity: CAT II

Vul ID: V-204519
Rule ID: SV-204519r603261_rule
STIG ID: RHEL-07-030390
Severity: CAT II

Vul ID: V-204520
Rule ID: SV-204520r603261_rule
STIG ID: RHEL-07-030400
Severity: CAT II

Vul ID: V-204521
Rule ID: SV-204521r603261_rule
STIG ID: RHEL-07-030410
Severity: CAT II

Vul ID: V-204522
Rule ID: SV-204522r603261_rule
STIG ID: RHEL-07-030420
Severity: CAT II

Vul ID: V-204523
Rule ID: SV-204523r603261_rule
STIG ID: RHEL-07-030430
Severity: CAT II

Vul ID: V-204524
 Rule ID: SV-204524r603261_rule
 STIG ID: RHEL-07-030440
 Severity: CAT II

Vul ID: V-204525
 Rule ID: SV-204525r603261_rule
 STIG ID: RHEL-07-030450
 Severity: CAT II

Vul ID: V-204526
 Rule ID: SV-204526r603261_rule
 STIG ID: RHEL-07-030460
 Severity: CAT II

Vul ID: V-204527
 Rule ID: SV-204527r603261_rule
 STIG ID: RHEL-07-030470
 Severity: CAT II

Vul ID: V-204528
 Rule ID: SV-204528r603261_rule
 STIG ID: RHEL-07-030480
 Severity: CAT II

Vul ID: V-204529
 Rule ID: SV-204529r603261_rule
 STIG ID: RHEL-07-030490
 Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	5.5 <u>Implement Automated Configuration Monitoring Systems</u> 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.			

4.1.3.13 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.

- The file `/var/log/lastlog` maintain records of the last time a user successfully logged in.
- The `/var/run/faillock/` directory maintains records of login failures via the `pam_faillock` module.

Note: Reloading the `auditd` config to set active settings requires the `auditd` service to be restarted, and may require a system reboot.

Rationale:

Monitoring login/logout events could provide a system administrator with information associated with brute force attacks against user logins.

Audit:

Run the following commands:

```
# grep logins /etc/audit/rules.d/*.rules
# auditctl -l | grep logins
```

Verify output of both includes:

```
-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`

Example: `vi /etc/audit/rules.d/50-logins.rules`

Add the following lines:

```
-w /var/log/lastlog -p wa -k logins
-w /var/run/faillock/ -p wa -k logins
```

References:

1. CCI: CCI-000126: The organization determines that the organization-defined subset of the auditable events defined in AU-2 are to be audited within the information system.
2. NIST SP 800-53 :: AU-2 d
3. NIST SP 800-53A :: AU-2.1 (v)
4. NIST SP 800-53 Revision 4 :: AU-2 d
5. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
6. NIST SP 800-53 :: AU-12 c
7. NIST SP 800-53A :: AU-12.1 (iv)
8. NIST SP 800-53 Revision 4 :: AU-12 c
9. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
10. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204540
Rule ID: SV-204540r603261_rule
STIG ID: RHEL-07-030610
Severity: CAT II

Vul ID: V-204541
Rule ID: SV-204541r603261_rule
STIG ID: RHEL-07-030620
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	4.9 <u>Log and Alert on Unsuccessful Administrative Account Login</u> Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.		●	●
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	16.13 <u>Alert on Account Login Behavior Deviation</u> Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.1.3.14 Ensure events that modify user/group information are collected (Automated)

Profile Applicability:

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

Description:

Record events affecting the `group`, `passwd` (user IDs), `shadow` and `gshadow` (passwords) or `/etc/security/opasswd` (old passwords, based on remember parameter in the PAM configuration) files. 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.

Note: Reloading the `auditd` config to set active settings may require a system reboot.

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:

Run the following command to check the `auditd .rules` files:

```
# grep identity /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
```

Run the following command to check loaded `auditd` rules:

```
# auditctl -l | grep identity
```

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
```

Remediation:

Edit or create a file in the `/etc/audit/rules.d/` directory ending in `.rules`

Example: `vi /etc/audit/rules.d/50-identity.rules`

Add the following lines:

```
-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
```

References:

1. CCI-000018: The information system automatically audits account creation actions
2. NIST SP 800-53 :: AC-2 (4)
3. NIST SP 800-53A :: AC-2 (4).1 (i&ii)
4. NIST SP 800-53 Revision 4 :: AC-2 (4)
5. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3
6. NIST SP 800-53 :: AU-12 c
7. NIST SP 800-53A :: AU-12.1 (iv)
8. NIST SP 800-53 Revision 4 :: AU-12 c
9. CCI-001403: The information system automatically audits account modification actions
10. NIST SP 800-53 :: AC-2 (4)
11. NIST SP 800-53A :: AC-2 (4).1 (i&ii)
12. NIST SP 800-53 Revision 4 :: AC-2 (4)
13. CCI-002130: The information system automatically audits account enabling actions
14. NIST SP 800-53 Revision 4 :: AC-2 (4)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204564
Rule ID: SV-204564r603261_rule
STIG ID: RHEL-07-030870
Severity: CAT II

Vul ID: V-204565
Rule ID: SV-204565r603261_rule
STIG ID: RHEL-07-030871
Severity: CAT II

Vul ID: V-204566
Rule ID: SV-204566r603261_rule
STIG ID: RHEL-07-030872
Severity: CAT II

Vul ID: V-204567
Rule ID: SV-204567r603261_rule
STIG ID: RHEL-07-030873
Severity: CAT II

Vul ID: V-204568
Rule ID: SV-204568r744115_rule
STIG ID: RHEL-07-030874
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			

4.1.3.15 Ensure all uses of the passwd command are audited. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the passwd command.

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 password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `passwd` command occur.

Check the file system rule in `/etc/audit/audit.rules` with the following command:

```
# grep -i /usr/bin/passwd /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/bin/passwd -F auid>=1000 -F auid!=4294967295 -k  
privileged-passwd
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `passwd` command occur.

Add or update the following rule in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Add, update or uncomment this line below

```
-a always,exit -F path=/usr/bin/passwd -F auid>=1000 -F auid!=4294967295 -k privileged-passwd
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI: CCI-000135: The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.
2. NIST SP 800-53 :: AU-3 (1)
3. NIST SP 800-53A :: AU-3 (1).1 (ii)
4. NIST SP 800-53 Revision 4 :: AU-3 (1)
5. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
6. NIST SP 800-53 :: AU-12 c
7. NIST SP 800-53A :: AU-12.1 (iv)
8. NIST SP 800-53 Revision 4 :: AU-12 c
9. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
10. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204542
Rule ID: SV-204542r603261_rule
STIG ID: RHEL-07-030630
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.16 Ensure auditing of the `unix_chkpwd` command (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the `unix_chkpwd` command.

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 password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `unix_chkpwd` command occur.

Check the file system rule in `/etc/audit/audit.rules` with the following command:

```
# grep -iw /usr/sbin/unix_chkpwd /etc/audit/audit.rules  
-a always,exit -F path=/usr/sbin/unix_chkpwd -F auid>=1000 -F  
auid!=4294967295 -k privileged-passwd
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `unix_chkpwd` command occur.

Add or update the following rule in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Add, uncomment or update this line:

```
-a always,exit -F path=/usr/sbin/unix_chkpwd -F auid>=1000 -F  
auid!=4294967295 -k privileged-passwd
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI: CCI-000135: The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.
2. NIST SP 800-53 :: AU-3 (1)
3. NIST SP 800-53A :: AU-3 (1).1 (ii)
4. NIST SP 800-53 Revision 4 :: AU-3 (1)
5. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
6. NIST SP 800-53 :: AU-12 c
7. NIST SP 800-53A :: AU-12.1 (iv)
8. NIST SP 800-53 Revision 4 :: AU-12 c
9. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
10. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204543
Rule ID: SV-204543r603261_rule
STIG ID: RHEL-07-030640
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.17 Ensure audit of the gpasswd command (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the gpasswd command.

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 password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the gpasswd command occur.

Check the file system rule in /etc/audit/audit.rules with the following command:

```
# grep -i /usr/bin/gpasswd /etc/audit/audit.rules  
-a always,exit -F path=/usr/bin/gpasswd -F auid>=1000 -F auid!=4294967295 -k  
privileged-passwd
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `gpasswd` command occur.

Add or update the following rule in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/bin/gpasswd -F auid>=1000 -F auid!=4294967295 -k privileged-passwd
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI: CCI-000135: The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.
2. NIST SP 800-53 :: AU-3 (1)
3. NIST SP 800-53A :: AU-3 (1).1 (ii)
4. NIST SP 800-53 Revision 4 :: AU-3 (1)
5. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
6. NIST SP 800-53 :: AU-12 c
7. NIST SP 800-53A :: AU-12.1 (iv)
8. NIST SP 800-53 Revision 4 :: AU-12 c
9. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
10. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204544
Rule ID: SV-204544r603261_rule
STIG ID: RHEL-07-030650
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.18 Ensure audit all uses of chage (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the chage command.

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 password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `chage` command occur.

Check the file system rule in `/etc/audit/audit.rules` with the following command:

```
# grep -i /usr/bin/chage /etc/audit/audit.rules  
-a always,exit -F path=/usr/bin/chage -F auid>=1000 -F auid!=4294967295 -k  
privileged-passwd
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `chage` command occur.

Add or update the following rule in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Add, uncomment or update the line:

```
-a always,exit -F path=/usr/bin/chage -F auid>=1000 -F auid!=4294967295 -k privileged-passwd
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI: CCI-000135: The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.
2. NIST SP 800-53 :: AU-3 (1)
3. NIST SP 800-53A :: AU-3 (1).1 (ii)
4. NIST SP 800-53 Revision 4 :: AU-3 (1)
5. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
6. NIST SP 800-53 :: AU-12 c
7. NIST SP 800-53A :: AU-12.1 (iv)
8. NIST SP 800-53 Revision 4 :: AU-12 c
9. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
10. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204545
Rule ID: SV-204545r603261_rule
STIG ID: RHEL-07-030660
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.19 Ensure audit all uses of the chsh command. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the chsh command.

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 access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `chsh` command occur.

Check that the following system call is being audited by performing the following command to check the file system rules in `/etc/audit/audit.rules`:

```
# grep -i /usr/bin/chsh /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/bin/chsh -F auid>=1000 -F auid!=4294967295 -k  
privileged-priv_change
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `chsh` command occur.

Add or update the following rule in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/bin/chsh -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI: CCI-000130: The information system generates audit records containing information that establishes what type of event occurred.
2. NIST SP 800-53 :: AU-3
3. NIST SP 800-53A :: AU-3.1
4. NIST SP 800-53 Revision 4 :: AU-3
5. CCI-000135: The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.
6. NIST SP 800-53 :: AU-3 (1)
7. NIST SP 800-53A :: AU-3 (1).1 (ii)
8. NIST SP 800-53 Revision 4 :: AU-3 (1)
9. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
10. NIST SP 800-53 :: AU-12 c
11. NIST SP 800-53A :: AU-12.1 (iv)
12. NIST SP 800-53 Revision 4 :: AU-12 c
13. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
14. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204551
Rule ID: SV-204551r603261_rule
STIG ID: RHEL-07-030720
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.20 Ensure audit the umount command (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the umount command.

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 mount commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `umount` command occur.

Check that the following system call is being audited by performing the following series of commands to check the file system rules in `/etc/audit/audit.rules`:

```
# grep -iw "/usr/bin/umount" /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/bin/umount -F auid>=1000 -F auid!=4294967295 -k  
privileged-mount
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `umount` command occur.

Add or update the following rule in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/bin/umount -F auid>=1000 -F auid!=4294967295 -k privileged-mount
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI: CCI-000135: The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.
2. NIST SP 800-53 :: AU-3 (1)
3. NIST SP 800-53A :: AU-3 (1).1 (ii)
4. NIST SP 800-53 Revision 4 :: AU-3 (1)
5. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
6. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204553
Rule ID: SV-204553r603261_rule
STIG ID: RHEL-07-030750
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.21 Ensure audit of postdrop command (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the postdrop command.

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 postfix commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `postdrop` command occur.

Check that the following system call is being audited by performing the following command to check the file system rules in `/etc/audit/audit.rules`:

```
# grep -iw /usr/sbin/postdrop /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/sbin/postdrop -F auid>=1000 -F auid!=4294967295 -  
k privileged-postfix
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `postdrop` command occur.

Add or update the following rule in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/sbin/postdrop -F auid>=1000 -F auid!=4294967295 -  
k privileged-postfix
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI: CCI-000135: The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.
2. NIST SP 800-53 :: AU-3 (1)
3. NIST SP 800-53A :: AU-3 (1).1 (ii)
4. NIST SP 800-53 Revision 4 :: AU-3 (1)
5. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
6. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204554
Rule ID: SV-204554r603261_rule
STIG ID: RHEL-07-030760
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.22 Ensure audit of postqueue command. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the postqueue command.

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 postfix commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `postqueue` command occur.

Check that the following system call is being audited by performing the following command to check the file system rules in `/etc/audit/audit.rules`:

```
# grep -iw /usr/sbin/postqueue /etc/audit/audit.rules
-a always,exit -F path=/usr/sbin/postqueue -F auid>=1000 -F auid!=4294967295
-k privileged-postfix
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `postqueue` command occur.

Add or update the following rule in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/sbin/postqueue -F auid>=1000 -F auid!=4294967295  
-k privileged-postfix
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI: CCI-000135: The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.
2. NIST SP 800-53 :: AU-3 (1)
3. NIST SP 800-53A :: AU-3 (1).1 (ii)
4. NIST SP 800-53 Revision 4 :: AU-3 (1)
5. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
6. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204555
Rule ID: SV-204555r603261_rule
STIG ID: RHEL-07-030770
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.23 Ensure audit ssh-keysign command. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the ssh-keysign command.

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 ssh commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `ssh-keysign` command occur.

Check that the following system call is being audited by performing the following command to check the file system rules in `/etc/audit/audit.rules`:

```
# grep -iw /usr/libexec/openssh/ssh-keysign /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/libexec/openssh/ssh-keysign -F auid>=1000 -F  
auid!=4294967295 -k privileged-ssh
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `ssh-keysign` command occur.

Add or update the following rule in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/libexec/openssh/ssh-keysign -F auid>=1000 -F auid!=4294967295 -k privileged-ssh
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI-000135: The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.
2. NIST SP 800-53 :: AU-3 (1)
3. NIST SP 800-53A :: AU-3 (1).1 (ii)
4. NIST SP 800-53 Revision 4 :: AU-3 (1)
5. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
6. NIST SP 800-53 :: AU-12 c
7. NIST SP 800-53A :: AU-12.1 (iv)
8. NIST SP 800-53 Revision 4 :: AU-12 c
9. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
10. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204556
Rule ID: SV-204556r603261_rule
STIG ID: RHEL-07-030780
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.24 Ensure audit of crontab command (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the crontab command.

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.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `crontab` command occur.

Check that the following system call is being audited by performing the following command to check the file system rules in `/etc/audit/audit.rules`:

```
# grep -iw /usr/bin/crontab /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/bin/crontab -F auid>=1000 -F auid!=4294967295 -k  
privileged-cron
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `crontab` command occur.

Add or update the following rule in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/bin/crontab -F auid>=1000 -F auid!=4294967295 -k privileged-cron
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI-000135: The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.
2. NIST SP 800-53 :: AU-3 (1)
3. NIST SP 800-53A :: AU-3 (1).1 (ii)
4. NIST SP 800-53 Revision 4 :: AU-3 (1)
5. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
6. NIST SP 800-53 :: AU-12 c
7. NIST SP 800-53A :: AU-12.1 (iv)
8. NIST SP 800-53 Revision 4 :: AU-12 c
9. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
10. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204557
Rule ID: SV-204557r603261_rule
STIG ID: RHEL-07-030800
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.25 Ensure audit of kmod command (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the kmod command.

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).

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `kmod` command occur.

Check the auditing rules in `/etc/audit/audit.rules` with the following command:

```
# grep -iw kmod /etc/audit/audit.rules  
-w /usr/bin/kmod -p x -F auid!=4294967295 -k module-change
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `kmod` command occur.

Add or update the following rule in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Add, uncomment or update the following line:

```
-w /usr/bin/kmod -p x -F auid!=4294967295 -k module-change
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3
2. NIST SP 800-53 :: AU-12 c
3. NIST SP 800-53A :: AU-12.1 (iv)
4. NIST SP 800-53 Revision 4 :: AU-12 c

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204563
Rule ID: SV-204563r603261_rule
STIG ID: RHEL-07-030840
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.26 Ensure audit of the rmdir syscall (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the rmdir syscall.

Rationale:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `rmdir` syscall occur.

Check the file system rules in `/etc/audit/audit.rules` with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

```
# grep -iw rmdir /etc/audit/audit.rules
-a always,exit -F arch=b32 -S rmdir -F auid>=1000 -F auid!=4294967295 -k
delete
-a always,exit -F arch=b64 -S rmdir -F auid>=1000 -F auid!=4294967295 -k
delete
```

If there are no audit rules defined for the `rmdir` syscall, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `rmdir` syscall occur.

Add the following rules in `/etc/audit/rules.d/audit.rules`:

Note: The rules are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be configured.

Example: `vim /etc/audit/rules.d/audit.rules`

Add, uncomment or update the following line that fits your system architecture:

```
-a always,exit -F arch=b32 -S rmdir -F auid>=1000 -F auid!=4294967295 -k delete
-a always,exit -F arch=b64 -S rmdir -F auid>=1000 -F auid!=4294967295 -k delete
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3
2. NIST SP 800-53 :: AU-12 c
3. NIST SP 800-53A :: AU-12.1 (iv)
4. NIST SP 800-53 Revision 4 :: AU-12 c
5. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events
6. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204571
Rule ID: SV-204571r603261_rule
STIG ID: RHEL-07-030900
Severity: CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.27 Ensure audit of unlink syscall (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the unlink syscall.

Rationale:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `unlink` syscall occur.

Check the file system rules in `/etc/audit/audit.rules` with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

```
# grep -iw unlink /etc/audit/audit.rules  
  
-a always,exit -F arch=b32 -S unlink -F auid>=1000 -F auid!=4294967295 -k  
delete  
-a always,exit -F arch=b64 -S unlink -F auid>=1000 -F auid!=4294967295 -k  
delete
```

If there are no audit rules defined for the `unlink` syscall, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `unlink` syscall occur.

Add the following rules in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Add, uncomment or update the following line depending on your system architecture:

Note: The rules are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be configured.

```
-a always,exit -F arch=b32 -S unlink -F auid>=1000 -F auid!=4294967295 -k delete
-a always,exit -F arch=b64 -S unlink -F auid>=1000 -F auid!=4294967295 -k delete
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3
2. NIST SP 800-53 :: AU-12 c
3. NIST SP 800-53A :: AU-12.1 (iv)
4. NIST SP 800-53 Revision 4 :: AU-12 c
5. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events
6. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204572
Rule ID: SV-204572r603261_rule
STIG ID: RHEL-07-030910
Severity: CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.28 Ensure audit unlinkat syscall (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the unlinkat syscall.

Rationale:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the unlinkat syscall occur.

Check the file system rules in `/etc/audit/audit.rules` with the following commands:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be present.

```
# grep -iw unlinkat /etc/audit/audit.rules
-a always,exit -F arch=b32 -S unlinkat -F auid>=1000 -F auid!=4294967295 -k
delete
-a always,exit -F arch=b64 -S unlinkat -F auid>=1000 -F auid!=4294967295 -k
delete
```

If there are no audit rules defined for the unlinkat syscall, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `unlinkat` syscall occur.

Add the following rules in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Add, uncomment, update the following line for the appropriate system architecture.

Note: The rules are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be configured.

```
-a always,exit -F arch=b32 -S unlinkat -F auid>=1000 -F auid!=4294967295 -k delete
-a always,exit -F arch=b64 -S unlinkat -F auid>=1000 -F auid!=4294967295 -k delete
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3
2. NIST SP 800-53 :: AU-12 c
3. NIST SP 800-53A :: AU-12.1 (iv)
4. NIST SP 800-53 Revision 4 :: AU-12 c
5. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events
6. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204573
Rule ID: SV-204573r603261_rule
STIG ID: RHEL-07-030920
Severity: CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.29 Ensure audit pam_timestamp_check command (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the pam_timestamp_check command.

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:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the pam_timestamp_check command occur.

Check the auditing rules in /etc/audit/audit.rules with the following command:

```
# grep -iw "/usr/sbin/pam_timestamp_check" /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/sbin/pam_timestamp_check -F auid>=1000 -F  
auid!=4294967295 -k privileged-pam
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the pam_timestamp_check command occur.

Add or update the following rule in /etc/audit/rules.d/audit.rules:

Example: vim /etc/audit/rules.d/audit.rules

Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/sbin/pam_timestamp_check -F auid>=1000 -F  
auid!=4294967295 -k privileged-pam
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
2. NIST SP 800-53 :: AU-12 c
3. NIST SP 800-53A :: AU-12.1 (iv)
4. NIST SP 800-53 Revision 4 :: AU-12 c

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204558
Rule ID: SV-204558r603261_rule
STIG ID: RHEL-07-030810
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.30 Ensure audit of the `finit_module` syscall (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the `finit_module` syscall.

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).

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `finit_module` syscall occur.

Check the auditing rules in `/etc/audit/audit.rules` with the following command:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the line appropriate for the system architecture must be present.

```
# grep -iw finit_module /etc/audit/audit.rules
-a always,exit -F arch=b32 -S finit_module -k module-change
-a always,exit -F arch=b64 -S finit_module -k module-change
```

If there are no audit rules defined for `finit_module`, refer to the remediation below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `finit_module` syscall occur.

Add or update the following rules in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Note: The rules are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be configured.

Add, uncomment or update the following line for the appropriate architecture:

```
-a always,exit -F arch=b32 -S finit_module -k module-change  
-a always,exit -F arch=b64 -S finit_module -k module-change
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3
2. NIST SP 800-53 :: AU-12 c
3. NIST SP 800-53A :: AU-12.1 (iv)
4. NIST SP 800-53 Revision 4 :: AU-12 c

Additional Information:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide  
Version 3, Release: 4 Benchmark Date: 23 Jul 2021  
  
Vul ID: V-204561  
Rule ID: SV-204561r603261_rule  
STIG ID: RHEL-07-030821  
Severity: CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.31 Ensure audit of the create_module syscall (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the create_module syscall.

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).

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the create_module syscall occur.

Check the auditing rules in /etc/audit/audit.rules with the following command:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the line appropriate for the system architecture must be present.

```
# grep -iw create_module /etc/audit/audit.rules  
-a always,exit -F arch=b32 -S create_module -k module-change  
-a always,exit -F arch=b64 -S create_module -k module-change
```

If there are no audit rules defined for create_module, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `create_module` syscall occur.

Add or update the following rules in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Note: The rules are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be configured.

Add, uncomment or update the following line appropriate for the architecture you are running.

```
-a always,exit -F arch=b32 -S create_module -k module-change
-a always,exit -F arch=b64 -S create_module -k module-change
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
2. NIST SP 800-53 :: AU-12 c
3. NIST SP 800-53A :: AU-12.1 (iv)
4. NIST SP 800-53 Revision 4 :: AU-12 c

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204559
Rule ID: SV-204559r603261_rule
STIG ID: RHEL-07-030819
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.32 Ensure auditing of all privileged functions (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all executions of privileged functions.

Rationale:

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse and identify the risk from insider threats and the advanced persistent threat.

Audit:

Verify the operating system audits the execution of privileged functions using the following command:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures.

Only the lines appropriate for the system architecture must be present.

```
# grep -iw execve /etc/audit/audit.rules

-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -k setuid
-a always,exit -F arch=b64 -S execve -C uid!=euid -F euid=0 -k setuid
-a always,exit -F arch=b32 -S execve -C gid!=egid -F egid=0 -k setgid
-a always,exit -F arch=b64 -S execve -C gid!=egid -F egid=0 -k setgid
```

If the audit rule for `SUID` files is not defined, refer to the remediation procedure below.

If the audit rule for `SGID` files is not defined, refer to the remediation procedure below.

Remediation:

Configure the operating system to audit the execution of privileged functions.

Add or update the following rule in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Note: The rules are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be configured.

```
-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -k setuid
-a always,exit -F arch=b64 -S execve -C uid!=euid -F euid=0 -k setuid
-a always,exit -F arch=b32 -S execve -C gid!=egid -F egid=0 -k setgid
-a always,exit -F arch=b64 -S execve -C gid!=egid -F egid=0 -k setgid
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI: CCI-002234: The information system audits the execution of privileged functions.
2. NIST SP 800-53 Revision 4 :: AC-6 (9)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204516
Rule ID: SV-204516r603261_rule
STIG ID: RHEL-07-030360
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.33 Ensure audit of semanage command (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the semanage command.

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).

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `semanage` command occur.

Check the file system rule in `/etc/audit/audit.rules` with the following command:

```
# grep -i /usr/sbin/semanage /etc/audit/audit.rules  
-a always,exit -F path=/usr/sbin/semanage -F auid>=1000 -F auid!=4294967295 -  
k privileged-priv_change
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `semanage` command occur.

Add or update the following rule in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/sbin/semanage -F auid>=1000 -F auid!=4294967295 -  
k privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI: CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
2. NIST SP 800-53 :: AU-12 c
3. NIST SP 800-53A :: AU-12.1 (iv)
4. NIST SP 800-53 Revision 4 :: AU-12 c
5. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
6. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204536
Rule ID: SV-204536r603261_rule
STIG ID: RHEL-07-030560
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.34 Ensure audit of the setsebool command. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the setsebool command.

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).

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `setsebool` command occur.

Check the file system rule in `/etc/audit/audit.rules` with the following command:

```
# grep -i /usr/sbin/setsebool /etc/audit/audit.rules  
-a always,exit -F path=/usr/sbin/setsebool -F auid>=1000 -F auid!=4294967295  
-k privileged-priv_change
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `setsebool` command occur.

Add or update the following rule in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/sbin/setsebool -F auid>=1000 -F auid!=4294967295  
-k privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI: CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
2. NIST SP 800-53 :: AU-12 c
3. NIST SP 800-53A :: AU-12.1 (iv)
4. NIST SP 800-53 Revision 4 :: AU-12 c
5. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
6. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204537
Rule ID: SV-204537r603261_rule
STIG ID: RHEL-07-030570
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.35 Ensure audit of the chcon command (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the chcon command.

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).

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `chcon` command occur.

Check the file system rule in `/etc/audit/audit.rules` with the following command:

```
# grep -i /usr/bin/chcon /etc/audit/audit.rules  
-a always,exit -F path=/usr/bin/chcon -F auid>=1000 -F auid!=4294967295 -k  
privileged-priv_change
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `chcon` command occur.

Add or update the following rule in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/bin/chcon -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI: CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
2. NIST SP 800-53 :: AU-12 c
3. NIST SP 800-53A :: AU-12.1 (iv)
4. NIST SP 800-53 Revision 4 :: AU-12 c
5. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
6. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204538
Rule ID: SV-204538r603261_rule
STIG ID: RHEL-07-030580
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.36 Ensure audit of the userhelper command (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the userhelper command.

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 password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `userhelper` command occur.

Check the file system rule in `/etc/audit/audit.rules` with the following command:

```
# grep -i /usr/sbin/userhelper /etc/audit/audit.rules
-a always,exit -F path=/usr/sbin/userhelper -F auid>=1000 -F auid!=4294967295
-k privileged-passwd
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `userhelper` command occur.

Add or update the following rule in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/sbin/userhelper -F auid>=1000 -F auid!=4294967295  
-k privileged-passwd
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI: CCI-000135: The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.
2. NIST SP 800-53 :: AU-3 (1)
3. NIST SP 800-53A :: AU-3 (1).1 (ii)
4. NIST SP 800-53 Revision 4 :: AU-3 (1)
5. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
6. NIST SP 800-53 :: AU-12 c
7. NIST SP 800-53A :: AU-12.1 (iv)
8. NIST SP 800-53 Revision 4 :: AU-12 c
9. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
10. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204546
Rule ID: SV-204546r603261_rule
STIG ID: RHEL-07-030670
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.37 Ensure audit of the mount command and syscall (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the mount command and syscall.

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 mount commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `mount` command and syscall occur.

Check that the following system call is being audited by performing the following series of commands to check the file system rules in `/etc/audit/audit.rules`:

```
# grep -iw "mount" /etc/audit/audit.rules

-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k
privileged-mount
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k
privileged-mount
-a always,exit -F path=/usr/bin/mount -F auid>=1000 -F auid!=4294967295 -k
privileged-mount
```

If all uses of the `mount` command and syscall are not being audited, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `mount` command and syscall occur.

Add or update the following rules in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Note: The rules are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be configured.

Add the following lines appropriate for the architecture:

```
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k privileged-mount
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k privileged-mount
-a always,exit -F path=/usr/bin/mount -F auid>=1000 -F auid!=4294967295 -k privileged-mount
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI: CCI-000135: The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.
2. NIST SP 800-53 :: AU-3 (1)
3. NIST SP 800-53A :: AU-3 (1).1 (ii)
4. NIST SP 800-53 Revision 4 :: AU-3 (1)
5. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
6. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204552
Rule ID: SV-204552r603261_rule
STIG ID: RHEL-07-030740
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.38 Ensure audit of the su command (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the su command.

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 access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `su` command occur.

Check that the following system call is being audited by performing the following command to check the file system rules in `/etc/audit/audit.rules`:

```
# grep -iw /usr/bin/su /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/bin/su -F auid>=1000 -F auid!=4294967295 -k  
privileged-priv_change
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `su` command occur.

Add or update the following rule in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Add the following line:

```
-a always,exit -F path=/usr/bin/su -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI: CCI-000130: The information system generates audit records containing information that establishes what type of event occurred.
2. NIST SP 800-53 :: AU-3
3. NIST SP 800-53A :: AU-3.1
4. NIST SP 800-53 Revision 4 :: AU-3
5. CCI-000135: The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.
6. NIST SP 800-53 :: AU-3 (1)
7. NIST SP 800-53A :: AU-3 (1).1 (ii)
8. NIST SP 800-53 Revision 4 :: AU-3 (1)
9. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
10. NIST SP 800-53 :: AU-12 c
11. NIST SP 800-53A :: AU-12.1 (iv)
12. NIST SP 800-53 Revision 4 :: AU-12 c
13. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
14. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204547
Rule ID: SV-204547r603261_rule
STIG ID: RHEL-07-030680
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.39 Ensure audit of setfiles command (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the setfiles command.

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).

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the `setfiles` command occur.

Check the file system rule in `/etc/audit/audit.rules` with the following command:

```
# grep -iw /usr/sbin/setfiles /etc/audit/audit.rules  
-a always,exit -F path=/usr/sbin/setfiles -F auid>=1000 -F auid!=4294967295 -  
k privileged-priv_change
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `setfiles` command occur.

Add or update the following rule in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/sbin/setfiles -F auid>=1000 -F auid!=4294967295 -  
k privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI: CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
2. NIST SP 800-53 :: AU-12 c
3. NIST SP 800-53A :: AU-12.1 (iv)
4. NIST SP 800-53 Revision 4 :: AU-12 c
5. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
6. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204539
Rule ID: SV-204539r603261_rule
STIG ID: RHEL-07-030590
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.40 Ensure audit all uses of the newgrp command (Automated)

Profile Applicability:

- STIG

Description:

The operating system must audit all uses of the newgrp command.

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 access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the newgrp command occur.

Check that the following system call is being audited by performing the following command to check the file system rules in /etc/audit/audit.rules:

```
# grep -i /usr/bin/newgrp /etc/audit/audit.rules  
  
-a always,exit -F path=/usr/bin/newgrp -F auid>=1000 -F auid!=4294967295 -k  
privileged-priv_change
```

If the command does not return any output, refer to the remediation procedure below.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the `newgrp` command occur.

Add or update the following rule in `/etc/audit/rules.d/audit.rules`:

Example: `vim /etc/audit/rules.d/audit.rules`

Add, uncomment or update the following line:

```
-a always,exit -F path=/usr/bin/newgrp -F auid>=1000 -F auid!=4294967295 -k privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

```
# service auditd restart
```

References:

1. CCI: CCI-000130: The information system generates audit records containing information that establishes what type of event occurred.
2. NIST SP 800-53 :: AU-3
3. NIST SP 800-53A :: AU-3.1
4. NIST SP 800-53 Revision 4 :: AU-3
5. CCI-000135: The information system generates audit records containing the organization-defined additional, more detailed information that is to be included in the audit records.
6. NIST SP 800-53 :: AU-3 (1)
7. NIST SP 800-53A :: AU-3 (1).1 (ii)
8. NIST SP 800-53 Revision 4 :: AU-3 (1)
9. CCI-000172: The information system generates audit records for the events defined in AU-2 d with the content defined in AU-3.
10. NIST SP 800-53 :: AU-12 c
11. NIST SP 800-53A :: AU-12.1 (iv)
12. NIST SP 800-53 Revision 4 :: AU-12 c
13. CCI-002884: The organization audits nonlocal maintenance and diagnostic sessions' organization-defined audit events.
14. NIST SP 800-53 Revision 4 :: MA-4 (1) (a)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204550
Rule ID: SV-204550r603261_rule
STIG ID: RHEL-07-030710
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

4.1.3.41 Ensure the audit configuration is immutable (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

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 "^s*[^#]" /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 following line at the end of the file:

```
-e 2
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

4.1.4 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.

4.1.4.1 Ensure Audit logs are owned by root and mode 0600 or less permissive (Automated)

Profile Applicability:

- STIG

Description:

The Linux operating system must protect audit information from unauthorized read, modification, or deletion.

Rationale:

If audit information were to become compromised, then forensic analysis and discovery of the true source of potentially malicious system activity is impossible to achieve.

To ensure the veracity of audit information, the operating system must protect audit information from unauthorized modification.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit information system activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029, SRG-OS-000206-GPOS-00084

Audit:

Verify the operating system audit records have proper permissions and ownership.

List the full permissions and ownership of the audit log files with the following command.

```
# ls -la /var/log/audit
total 4512
drwx-----. 2 root root 23 Apr 25 16:53 .
drwxr-xr-x. 17 root root 4096 Aug 9 13:09 ..
-rw-----. 1 root root 8675309 Aug 9 12:54 audit.log
```

Audit logs must be mode 0600 or less permissive.

If any are more permissive, this is a finding.

The owner and group owner of all audit log files must both be "root". If any other owner or group owner is listed, this is a finding.

Remediation:

Change the mode of the audit log files with the following command:

```
# chmod 0600 [audit_file]
```

Change the owner and group owner of the audit log files with the following command:

```
# chown root:root [audit_file]
```

References:

1. CCI-000162: The information system protects audit information from unauthorized access
2. NIST SP 800-53 :: AU-9
3. NIST SP 800-53A :: AU-9.1
4. NIST SP 800-53 Revision 4 :: AU-9
5. CCI-000163: The information system protects audit information from unauthorized modification.
6. NIST SP 800-53 :: AU-9
7. NIST SP 800-53A :: AU-9.1
8. NIST SP 800-53 Revision 4 :: AU-9
9. CCI-000164: The information system protects audit information from unauthorized deletion.
10. NIST SP 800-53 :: AU-9
11. NIST SP 800-53A :: AU-9.1
12. NIST SP 800-53 Revision 4 :: AU-9
13. CCI-001314: The information system reveals error messages only to organization-defined personnel or roles
14. NIST SP 800-53 :: SI-11 c
15. NIST SP 800-53A :: SI-11.1 (iv)
16. NIST SP 800-53 Revision 4 :: SI-11 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-228564
Rule ID: SV-228564r606407_rule
STIG ID: RHEL-07-910055
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

4.2 Configure 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 and ease log analysis.

4.2.1 Configure rsyslog

The `rsyslog` software is recommended as a replacement for the `syslogd` daemon and provides improvements over `syslogd`, 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.

Notes:

- *This section only applies if `rsyslog` is installed on the system*
- *If another logging software like `syslog-ng` is in use on the system:*
 - *This section may be skipped*
 - *Ensure that logging software is configured in accordance with local site policy*

4.2.1.1 Ensure rsyslog is installed (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `rsyslog` software is a recommended replacement to the original `syslogd` daemon.

`rsyslog` provides improvements over `syslogd`, including:

- connection-oriented (i.e. TCP) transmission of logs
- The option to log to database formats
- Encryption of log data en route to a central logging server

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:

Run the following command to Verify `rsyslog` is installed:

```
# rpm -q rsyslog  
rsyslog-<version>
```

Remediation:

Run the following command to install `rsyslog`:

```
# yum install rsyslog
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

4.2.1.2 Ensure rsyslog Service is enabled and running (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`rsyslog` needs to be enabled and running to perform logging

Rationale:

If the `rsyslog` service is not activated the system may default to the `syslogd` service or lack logging instead.

Audit:

Run one of the following commands to verify `rsyslog` is enabled:

```
# systemctl is-enabled rsyslog
enabled
```

Run the following command to verify that `rsyslog` is running:

```
# systemctl status rsyslog | grep 'active (running) '
Active: active (running) since <Day date time>
```

Remediation:

Run the following command to enable and start `rsyslog`:

```
# systemctl --now enable rsyslog
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

4.2.1.3 Ensure rsyslog default file permissions configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`rsyslog` will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

The `$FileCreateMode` parameter specifies the file creation mode with which `rsyslogd` creates new files. If not specified, the value `0644` is used.

Notes:

- *The value given must always be a 4-digit octal number, with the initial digit being zero.*
- *This setting can be overridden by a less restrictive setting in any file ending in `.conf` in the `/etc/rsyslog.d/` directory*

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 and verify that `$FileCreateMode` is `0640` or more restrictive:

```
# grep ^\$FileCreateMode /etc/rsyslog.conf /etc/rsyslog.d/*.conf
$FileCreateMode 0640
```

Verify that no results return with a less restrictive file mode

Remediation:

Edit the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and set `$FileCreateMode` to `0640` or more restrictive:

```
$FileCreateMode 0640
```

References:

1. See the rsyslog.conf(5) man page for more information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

4.2.1.4 Ensure logging is configured (Manual)

Profile Applicability:

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

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 the `/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:

```
# 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:

```
*.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
news.crit                              -/var/log/news/news.crit
news.err                              -/var/log/news/news.err
news.notice                           -/var/log/news/news.notice
*.=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. CCI: CCI-000366: The organization implements the security configuration settings.
3. NIST SP 800-53 :: CM-6 b
4. NIST SP 800-53A :: CM-6.1 (iv)
5. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204489
Rule ID: SV-204489r744109_rule
STIG ID: RHEL-07-021100
Severity: CAT II
```


CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

4.2.1.5 Ensure rsyslog is configured to send logs to a remote log host (Automated)

Profile Applicability:

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

Description:

The `rsyslog` utility supports the ability to send logs it gathers to a remote log host running `syslogd(8)` or to receive messages from remote hosts, reducing administrative overhead.

Note: Ensure that the selection of logfiles being sent follows local site policy

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.

```
# grep -E '^s*([^\#]+\s+)?action\((([^\#]+\s+)?\btarget=\"?[^\"]+\"?\b' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Output should include `target=<FQDN or IP of remote loghost>`

OR

```
# grep -E '^[^\#]\s*\S+\.\.*\s+@' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Output should include either the FQDN or the IP of the remote loghost

Remediation:

Edit the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and add one of the following lines:

Newer syntax:

```
<files to sent to the remote log server> action(type="omfwd" target="<FQDN or  
ip of loghost>" port="<port number>" protocol="tcp"  
  
action.resumeRetryCount="<number of re-tries>"  
queue.type="LinkedList"  
queue.size="<number of messages to queue>")
```

Example:

```
*.* action(type="omfwd" target="192.168.2.100" port="514" protocol="tcp"  
        action.resumeRetryCount="100"  
        queue.type="LinkedList" queue.size="1000")
```

Older syntax:

```
*.* @@<FQDN or ip of loghost>
```

Example:

```
*.* @@192.168.2.100
```

Run the following command to reload the `rsyslog` configuration:

```
# systemctl restart rsyslog
```

References:

1. See the `rsyslog.conf(5)` man page for more information.
2. CCI-000366: The organization implements the security configuration settings
3. NIST SP 800-53 :: CM-6 b
4. NIST SP 800-53A :: CM-6.1 (iv)
5. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

The double "at" sign (@@) directs `rsyslog` to use TCP to send log messages to the server, which is a more reliable transport mechanism than the default UDP protocol

The *. * is a "wildcard" to send all logs to the remote loghost

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204574
Rule ID: SV-204574r603261_rule
STIG ID: RHEL-07-031000
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.			
v7	6.6 Deploy SIEM or Log Analytic tool Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.			
v7	6.8 Regularly Tune SIEM On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.			

4.2.1.6 Ensure remote rsyslog messages are only accepted on designated log hosts. (Manual)

Profile Applicability:

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

Description:

By default, `rsyslog` does not listen for log messages coming in from remote systems. The `ModLoad` tells `rsyslog` to load the `imtcp.so` module so it can listen over a network via TCP. The `InputTCPServerRun` option instructs `rsyslogd` to listen on the specified TCP port.

Note: The `$ModLoad imtcp` line can have the `.so` extension added to the end of the module, or use the full path to the module.

Rationale:

The guidance in the section ensures that remote log hosts are configured to only accept `rsyslog` data from hosts within the specified domain and that those systems that are not designed to be log hosts do not accept any remote `rsyslog` messages. This provides protection from spoofed log data and ensures that system administrators are reviewing reasonably complete syslog data in a central location.

Audit:

Run the following commands and verify the resulting lines are uncommented on designated log hosts and commented or removed on all others:

```
# grep '$ModLoad imtcp' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
$ModLoad imtcp
# grep '$InputTCPServerRun' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
$InputTCPServerRun 514
```

Remediation:

For hosts that are designated as log hosts, edit the `/etc/rsyslog.conf` file and uncomment or add the following lines:

```
$ModLoad imtcp
$InputTCPServerRun 514
```

For hosts that are not designated as log hosts, edit the `/etc/rsyslog.conf` file and comment or remove the following lines:

```
# $ModLoad imtcp
# $InputTCPServerRun 514
```

Run the following command to reload the `rsyslogd` configuration:

```
# systemctl restart rsyslog
```

References:

1. See the `rsyslog(8)` man page for more information.
2. CCI-000318: The organization audits and reviews activities associated with configuration controlled changes to the system
3. NIST SP 800-53 :: CM-3 e
4. NIST SP 800-53A :: CM-3.1 (v)
5. NIST SP 800-53 Revision 4 :: CM-3 f
6. CCI-000368: The organization documents any deviations from the established configuration settings for organization-defined information system components based on organization-defined operational requirements
7. NIST SP 800-53 :: CM-6 c
8. NIST SP 800-53A :: CM-6.1 (v)
9. NIST SP 800-53 Revision 4 :: CM-6 c
10. CCI-001812: The information system prohibits user installation of software without explicit privileged status
11. NIST SP 800-53 Revision 4 :: CM-11 (2)
12. CCI-001813: The information system enforces access restrictions
13. NIST SP 800-53 Revision 4 :: CM-5 (1)
14. CCI-001814: The Information system supports auditing of the enforcement actions
15. NIST SP 800-53 Revision 4 :: CM-5 (1)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204575
Rule ID: SV-204575r603261_rule
STIG ID: RHEL-07-031010
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4.2.2 Configure journald

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

Note: Any changes made to the systemd-journald configuration will require a re-start of systemd-journald

4.2.2.1 Ensure journald is configured to send logs to rsyslog (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. Utilities exist to accept remote export of journald logs, however, use of the rsyslog service provides a consistent means of log collection and export.

Notes:

- *This recommendation assumes that recommendation 4.2.1.5, "Ensure rsyslog is configured to send logs to a remote log host" has been implemented.*
- *The main configuration file `/etc/systemd/journald.conf` is read before any of the custom `*.conf` files. If there are custom configs present, they override the main configuration parameters*
- *As noted in the journald man pages: 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.*

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 `/etc/systemd/journald.conf` and verify that logs are forwarded to syslog

```
# grep -E ^\s*ForwardToSyslog /etc/systemd/journald.conf
ForwardToSyslog=yes
```

Remediation:

Edit the `/etc/systemd/journald.conf` file and add the following line:

```
ForwardToSyslog=yes
```

References:

1. <https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemdjournaldconf>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.			
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.			

4.2.2.2 Ensure journald is configured to compress large log files (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.

Note: The main configuration file `/etc/systemd/journald.conf` is read before any of the custom `*.conf` files. If there are custom configs present, they override the main configuration parameters

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:

Review `/etc/systemd/journald.conf` and verify that large files will be compressed:

```
# grep -E ^\s*Compress /etc/systemd/journald.conf
Compress=yes
```

Remediation:

Edit the `/etc/systemd/journald.conf` file and add the following line:

```
Compress=yes
```

References:

1. <https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemdjournaldconf>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> 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> Ensure that all systems that store logs have adequate storage space for the logs generated.			

4.2.2.3 Ensure journald is configured to write logfiles to persistent disk (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.

Note: The main configuration file `/etc/systemd/journald.conf` is read before any of the custom `*.conf` files. If there are custom configs present, they override the main configuration parameters

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:

Review `/etc/systemd/journald.conf` and verify that logs are persisted to disk:

```
# grep -E ^\s*Storage /etc/systemd/journald.conf
Storage=persistent
```

Remediation:

Edit the `/etc/systemd/journald.conf` file and add the following line:

```
Storage=persistent
```

References:

1. <https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemdjournaldconf>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

4.2.3 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`.

Note: If no `maxage` setting is set for logrotate a situation can occur where logrotate is interrupted and fails to delete rotated logfiles. 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 logfile is removed but standard rotation settings are not overridden.

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> 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> Ensure that all systems that store logs have adequate storage space for the logs generated.			

4.2.4 Ensure permissions on all logfiles are configured (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Log files stored in /var/log/ contain logged information from many services on the system, or on log hosts others as well.

Rationale:

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected. Other/world should not have the ability to view this information. Group should not have the ability to modify this information.

Audit:

Run the following command and verify that other has no permissions on any files and group does not have write or execute permissions on any files:

```
# find /var/log -type f -perm /g+wx,o+rw -exec ls -l {} \;
```

Nothing should be returned

Remediation:

Run the following commands to set permissions on all existing log files:

```
# find /var/log -type f -exec chmod g-wx,o-rwx "{}" +
```

Note: The configuration for your logging software or services may need to also be modified for any logs that had incorrect permissions, otherwise, the permissions may be reverted to the incorrect permissions

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

5 Access, Authentication and Authorization

- Access - Access control for an operating system determines how the operating system implements accesses to system resources by satisfying the security objectives of integrity, availability, and secrecy
- Authentication - Authentication is the process of recognizing a user's identity
- Authorization - Authorization is a security mechanism to determine access levels or user/client privileges related to system resources including files, services, computer programs, data and application features

5.1 Configure time-based job schedulers

`cron` is a time-based job scheduler used to schedule jobs, commands or shell scripts, to run periodically at fixed times, dates, or intervals.

`at` provides the ability to execute a command or shell script at a specified date and hour, or after a given interval of time.

Other methods exist for scheduling jobs, such as `systemd` timers. If another method is used, it should be secured in accordance with local site policy

Note: `systemd` timers are `systemd` unit files whose name ends in `.timer` that control `.service` files or events. Timers can be used as an alternative to `cron` and `at`. Timers have built-in support for calendar time events, monotonic time events, and can be run asynchronously

If `cron` and `at` are not installed, this section can be skipped.

5.1.1 Ensure cron daemon is enabled and running (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. If another method for scheduling tasks is not being used, `cron` is used to execute them, and needs to be enabled and running.

Audit:

If `cron` is installed:

Run the following commands to verify `cron` is enabled and running:

```
# systemctl is-enabled crond  
  
enabled  
# systemctl status crond | grep 'Active: active (running) '  
  
Active: active (running) since <Day Date Time>
```

Remediation:

Run the following command to enable and start `cron`:

```
# systemctl --now enable crond
```

OR

Run the following command to remove `cron`:

```
# yum remove cronie
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

5.1.2 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:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat /etc/crontab
Access: (0600/-rw-----)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/crontab`:

```
# chown root:root /etc/crontab
# chmod u-x,og-rwx /etc/crontab
```

OR

Run the following command to remove `cron`:

```
# yum remove cronie
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

5.1.3 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:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other` :

```
# stat /etc/cron.hourly/
Access: (0700/drwx-----)  Uid: (    0/    root)  Gid: (    0/    root)
```

Remediation:

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/
```

OR

Run the following command to remove `cron`

```
# yum remove cronie
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

5.1.4 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:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other` :

```
# stat /etc/cron.daily/  
Access: (0700/drwx-----)  Uid: (    0/    root)  Gid: (    0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/cron.daily` directory:

```
# chown root:root /etc/cron.daily
# chmod og-rwx /etc/cron.daily
```

OR

Run the following command to remove `cron`:

```
# yum remove cronie
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

5.1.5 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

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other` :

```
# stat /etc/cron.weekly
Access: (0700/drwx-----)  Uid: (    0/    root)  Gid: (    0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/cron.weekly/` directory:

```
# chown root:root /etc/cron.weekly/  
# chmod og-rwx /etc/cron.weekly/
```

OR

Run the following command to remove `cron`:

```
# yum remove cronie
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

5.1.6 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:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat /etc/cron.monthly/  
Access: (0700/drwx-----)  Uid: (    0/    root)  Gid: (    0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/cron.monthly` directory:

```
# chown root:root /etc/cron.monthly
# chmod og-rwx /etc/cron.monthly
```

OR

Run the following command to remove `cron`:

```
# yum remove cronie
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

5.1.7 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:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other` :

```
# stat /etc/cron.d
Access: (0700/drwx-----)  Uid: (    0/    root)  Gid: (    0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/cron.d` directory:

```
# chown root:root /etc/cron.d
# chmod og-rwx /etc/cron.d
```

OR

Run the following command to remove `cron`:

```
# yum remove cronie
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

5.1.8 Ensure cron is restricted to authorized users (Automated)

Profile Applicability:

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

Description:

If `cron` is installed in the system, configure `/etc/cron.allow` to allow specific users to use these services. If `/etc/cron.allow` does not exist, then `/etc/cron.deny` is checked. Any user not specifically defined in those files is allowed to use cron. By removing the file, only users in `/etc/cron.allow` are allowed to use cron.

Note: Even though a given user is not listed in `cron.allow`, cron jobs can still be run as that user. The `cron.allow` file 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:

Run the following command and verify `/etc/cron.deny` does not exist:

```
# stat /etc/cron.deny
stat: cannot stat `/etc/cron.deny': No such file or directory
```

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other` for `/etc/cron.allow`:

```
# stat /etc/cron.allow
Access: (0600/-rw-----)  Uid: (   0/   root)  Gid: (   0/   root)
```

Remediation:

Run the following command to remove `/etc/cron.deny`:

```
# rm /etc/cron.deny
```

Run the following command to create `/etc/cron.allow`

```
# touch /etc/cron.allow
```

Run the following commands to set the owner and permissions on `/etc/cron.allow`:

```
# chown root:root /etc/cron.allow  
# chmod u-x,og-rwx /etc/cron.allow
```

OR

Run the following command to remove `cron`

```
# yum remove cronie
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204490
Rule ID: SV-204490r603261_rule
STIG ID: RHEL-07-021110
Severity: CAT II

Vul ID: V-204491
Rule ID: SV-204491r603261_rule
STIG ID: RHEL-07-021120
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	16 <u>Account Monitoring and Control</u> Account Monitoring and Control			

5.1.9 Ensure at is restricted to authorized users (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

If `at` is installed in the system, configure `/etc/at.allow` to allow specific users to use these services. If `/etc/at.allow` does not exist, then `/etc/at.deny` is checked. Any user not specifically defined in those files is allowed to use `at`. By removing the file, only users in `/etc/at.allow` are allowed to use `at`.

Note: Even though a given user is not listed in `at.allow`, `at` jobs can still be run as that user. The `at.allow` file only controls administrative access to the `at` command for scheduling and modifying `at` jobs.

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:

Run the following command and verify `/etc/at.deny` does not exist:

```
# stat /etc/at.deny
stat: cannot stat `/etc/at.deny': No such file or directory
```

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other` for `/etc/at.allow`:

```
# stat /etc/at.allow
Access: (0600/-rw-----)  Uid: (    0/    root)  Gid: (    0/    root)
```

Remediation:

Run the following command to remove `/etc/at.deny`:

```
# rm /etc/at.deny
```

Run the following command to create `/etc/at.allow`

```
# touch /etc/at.allow
```

Run the following commands to set the owner and permissions on `/etc/at.allow`:

```
# chown root:root /etc/at.allow
# chmod u-x,og-rwx /etc/at.allow
```

OR

Run the following command to remove `at`:

```
# yum remove at
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	16 <u>Account Monitoring and Control</u> Account Monitoring and Control			

5.2 Configure sudo

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.

sudo supports a plugin architecture for security policies and input/output logging. Third parties can develop and distribute their own policy and I/O logging plugins to work seamlessly with the sudo front end. The default security policy is sudoers, which is configured via the file `/etc/sudoers`.

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 plugin architecture for security policies and input/output logging. Third parties can develop and distribute their own policy and I/O logging plugins to work seamlessly with the sudo front end. The default security policy is sudoers, which is configured via the file /etc/sudoers.

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:

```
# rpm -q sudo  
sudo-<VERSION>
```

Remediation:

Run the following command to install sudo.

```
# yum install sudo
```

References:

1. SUDO(8)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	4 <u>Controlled Use of Administrative Privileges</u> Controlled Use of Administrative Privileges			

5.2.2 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-pty

Note: 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. The -f option allows you to tell visudo which file to edit.

Rationale:

Attackers can run a malicious program using sudo, which would again fork a background process that remains even when the main program has finished executing.

This can be mitigated by configuring sudo to run other commands only from a pseudo-pty, whether I/O logging is turned on or not.

Audit:

Verify that sudo can only run other commands from a pseudo-pty

Run the following command:

```
# grep -Ei '^s*Defaults\s+([\^#\]\S+,\s*)?use_pty\b' /etc/sudoers
/etc/sudoers.d/*

Defaults use_pty
```

Remediation:

Edit the file /etc/sudoers or a file in /etc/sudoers.d/ with visudo or visudo -f <PATH TO FILE> and add the following line:

```
Defaults use_pty
```

References:

1. SUDO(8)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	4 <u>Controlled Use of Administrative Privileges</u> Controlled Use of Administrative Privileges			

5.2.3 Ensure sudo log file exists (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

sudo can use a custom log file

Note: 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. The -f option allows you to tell visudo which file to edit.

Rationale:

A sudo log file simplifies auditing of sudo commands

Impact:

Editing the sudo configuration incorrectly can cause sudo to stop functioning

Audit:

Verify that sudo has a custom log file configured

Run the following command:

```
# grep -Ei '^\\s*Defaults\\s+([\\^#;]+,\\s*)?logfile\\s*=\\s*("[^#;]+")?'  
/etc/sudoers /etc/sudoers.d/*  
  
Defaults logfile="/var/log/sudo.log"
```

Remediation:

edit the file /etc/sudoers or a file in /etc/sudoers.d/ with visudo or visudo -f <PATH TO FILE> and add the following line:

```
Defaults logfile "<PATH TO CUSTOM LOG FILE>"
```

Example:

```
Defaults logfile="/var/log/sudo.log"
```

References:

1. SUDO(8)
2. VISUDO(8)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

5.2.4 Ensure users must provide password for escalation (Automated)

Profile Applicability:

- 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.

Audit:

***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 -i nopasswd /etc/sudoers /etc/sudoers.d/*
```

If any uncommented line is found with a `NOPASSWD` tag, refer to the remediation procedure below.

Remediation:

Configure the operating system to require users to supply a password for privilege escalation.

Check the configuration of the `/etc/sudoers` file with the following command:

```
# vim /etc/sudoers
```

Remove any occurrences of `NOPASSWD` tags in the file.

Check the configuration of the `/etc/sudoers.d/*` files with the following command to get the list:

```
# grep -i nopasswd /etc/sudoers.d/*
```

Edit the list of files using this command:

```
# vim /etc/sudoers.d/path_of_file
```

Remove any occurrences of `NOPASSWD` tags in the file.

References:

1. CCI-002038: The organization requires users to reauthenticate when organization-defined circumstances or situations requiring reauthentication.
2. NIST SP 800-53 Revision 4 :: IA-11

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204429
Rule ID: SV-204429r603261_rule
STIG ID: RHEL-07-010340
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> 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	<u>4.3 Ensure the Use of Dedicated Administrative Accounts</u> 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.			

5.2.5 Ensure users must re-authenticate for privilege escalation (Automated)

Profile Applicability:

- 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 reauthenticate for privilege escalation. Check the configuration of the `/etc/sudoers` and `/etc/sudoers.d/*` files with the following command:

```
# grep -i authenticate /etc/sudoers /etc/sudoers.d/*
```

If any uncommented 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.
Check the configuration of the `/etc/sudoers` file with the following command:

```
# vim /etc/sudoers
```

Remove any occurrences of `!authenticate` tags in the file.

Check the configuration of the `/etc/sudoers.d/*` files with the following command:

```
# grep -i authenticate /etc/sudoers /etc/sudoers.d/*
```

Edit the list of files using this command:

```
# vim /etc/sudoers.d/{path_of_file}
```

Remove any occurrences of `!authenticate` tags in the file(s).

References:

1. CI-002038: The organization requires users to reauthenticate when organization-defined circumstances or situations requiring reauthentication
2. NIST SP 800-53 Revision 4 :: IA-11

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204430
Rule ID: SV-204430r603261_rule
STIG ID: RHEL-07-010350
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> 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	<u>4.3 Ensure the Use of Dedicated Administrative Accounts</u> 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 Linux 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. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-237633
Rule ID: SV-237633r646850_rule
STIG ID: RHEL-07-010341
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> 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	<u>4.3 Ensure the Use of Dedicated Administrative Accounts</u> 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 sudo authentication timeout is configured (Automated)

Profile Applicability:

- STIG

Description:

The Linux operating system must require re-authentication when using the "sudo" command.

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 organization requires the user to re-authenticate when using the "sudo" command.

If the value is set to an integer less than 0, the user's time stamp will not expire and the user will not have to re-authenticate for privileged actions until the user's session is terminated.

Audit:

Verify the operating system requires re-authentication when using the "sudo" command to elevate privileges.

```
# grep -i 'timestamp_timeout' /etc/sudoers /etc/sudoers.d/*  
  
/etc/sudoers:Defaults timestamp_timeout=0
```

If "timestamp_timeout" is set to a negative number, is commented out, or no results are returned, this is a finding.

Remediation:

Configure the "sudo" command to require re-authentication.

Edit the /etc/sudoers file:

```
# visudo
```

Add or modify the following line:

```
Defaults timestamp_timeout=[value]
```

Note: The "[value]" must be a number that is greater than or equal to "0".

References:

1. <https://www.sudo.ws/man/1.9.0/sudoers.man.html>
2. CCI-002038: The organization requires users to reauthenticate when organization-defined circumstances or situations requiring reauthentication
3. NIST SP 800-53 Revision 4 :: IA-11

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-237635
Rule ID: SV-237635r646856_rule
STIG ID: RHEL-07-010343
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> 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	4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u> 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 users password required for privilege escalation when using sudo (Automated)

Profile Applicability:

- STIG

Description:

The Linux 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.

```
# egrep -i '(!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
```

References:

1. CCI-002227: The organization restricts privileged accounts on the information system to organization-defined personnel or roles
2. NIST SP 800-53 Revision 4 :: AC-6 (5)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-237634
Rule ID: SV-237634r646853_rule
STIG ID: RHEL-07-010342
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> 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	<u>4.3 Ensure the Use of Dedicated Administrative Accounts</u> 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 Configure SSH Server

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.

Note:

- 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.
 - Command to remove the SSH daemon:

```
# yum remove openssh-server
```

- Once all configuration changes have been made to `/etc/ssh/sshd_config`, the `sshd` configuration must be reloaded:
 - Command to re-load the SSH daemon configuration:

```
# systemctl reload sshd
```

5.3.1 Ensure SSH is installed (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that all networked systems 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, logical means (cryptography) do not have to be employed, and vice versa.

Audit:

Check to see if `sshd` is installed with the following command:

```
# yum list installed \*ssh\*  
  
libssh2.x86_64 1.4.3-8.el7 @anaconda/7.1  
openssh.x86_64 6.6.1p1-11.el7 @anaconda/7.1  
openssh-server.x86_64 6.6.1p1-11.el7 @anaconda/7.1
```

If the `SSH server` package is not installed, refer to the remediation procedure below.

Remediation:

Install SSH packages onto the host with the following commands:

```
# yum install openssh-server
```

References:

1. CCI-002418: The information system protects the confidentiality and/or integrity of transmitted information
2. NIST SP 800-53 Revision 4 :: SC-8
3. CCI-002420: The information system maintains the confidentiality and/or integrity of information during preparation for transmission
4. NIST SP 800-53 Revision 4 :: SC-8 (2)
5. CCI-002421: The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by organization-defined alternative physical safeguards
6. NIST SP 800-53 Revision 4 :: SC-8 (1)
7. CCI-002422: The information system maintains the confidentiality and/or integrity of information during reception
8. NIST SP 800-53 Revision 4 :: SC-8 (2)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204585
Rule ID: SV-204585r603261_rule
STIG ID: RHEL-07-040300
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> 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> Encrypt all sensitive information in transit.			

5.3.2 Ensure SSH is running (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that all networked systems use SSH for 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.

Audit:

Verify `SSH` is loaded and active with the following command:

```
# systemctl status sshd

sshd.service - OpenSSH server daemon
Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled)
Active: active (running) since Tue 2015-11-17 15:17:22 EST; 4 weeks 0 days ago
Main PID: 1348 (sshd)
CGroup: /system.slice/ssh.service
1053 /usr/sbin/sshd -D
```

If `sshd` does not show a status of `active` and `running`, refer to the remediation procedure below.

Remediation:

Configure the `SSH` service to start and automatically start after reboot with the following command:

```
# systemctl --now enable sshd.service
```

References:

1. CCI-002418: The information system protects the confidentiality and/or integrity of transmitted information
2. NIST SP 800-53 Revision 4 :: SC-8
3. CCI-002420: The information system maintains the confidentiality and/or integrity of information during preparation for transmission
4. NIST SP 800-53 Revision 4 :: SC-8 (2)
5. CCI-002421: The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by organization-defined alternative physical safeguards
6. NIST SP 800-53 Revision 4 :: SC-8 (1)
7. CCI-002422: The information system maintains the confidentiality and/or integrity of information during reception
8. NIST SP 800-53 Revision 4 :: SC-8 (2)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204586
Rule ID: SV-204586r603261_rule
STIG ID: RHEL-07-040310
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.			

5.3.3 Ensure permissions on /etc/ssh/sshd_config are configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `/etc/ssh/sshd_config` file contains configuration specifications for `sshd`. The command below sets the owner and group of the file to `root`.

Rationale:

The `/etc/ssh/sshd_config` file needs to be protected from unauthorized changes by non-privileged users.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat /etc/ssh/sshd_config
Access: (0600/-rw-----)  Uid: (  0/   root)  Gid: (  0/   root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/ssh/sshd_config`:

```
# chown root:root /etc/ssh/sshd config
# chmod og-rwx /etc/ssh/sshd_config
```

Default Value:

Access: (0600/-rw-----) Uid: (0/ root) Gid: (0/ root)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

5.3.4 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 command and verify Uid is 0/root and Gid is either 0/root or {gid}/ssh_keys and permissions are 0640 or more restrictive:

```
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec stat {} \;
```

Example Output:

```
File: /etc/ssh/ssh_host_ed25519_key
Size: 387          Blocks: 8          IO Block: 4096   regular file
Device: fd00h/64768d Inode: 35440357    Links: 1
Access: (0640/-rw-r-----) Uid: ( 0/   root)   Gid: ( 994/ssh_keys)
Context: system_u:object_r:sshd_key_t:s0
Access: 2021-11-08 13:25:26.109417596 -0500
Modify: 2021-08-12 13:26:20.839744186 -0400
Change: 2021-08-12 13:26:20.873744187 -0400
Birth: -
File: /etc/ssh/ssh_host_ecdsa_key
Size: 480          Blocks: 8          IO Block: 4096   regular file
Device: fd00h/64768d Inode: 35440364    Links: 1
Access: (0640/-rw-r-----) Uid: ( 0/   root)   Gid: ( 994/ssh_keys)
Context: system_u:object_r:sshd_key_t:s0
Access: 2021-11-08 13:25:26.108417589 -0500
Modify: 2021-08-12 13:26:21.368353670 -0400
Change: 2021-08-12 13:26:21.457353673 -0400
Birth: -
File: /etc/ssh/ssh_host_rsa_key
Size: 2578         Blocks: 8          IO Block: 4096   regular file
Device: fd00h/64768d Inode: 35440373    Links: 1
Access: (0640/-rw-r-----) Uid: ( 0/   root)   Gid: ( 994/ssh_keys)
Context: system_u:object_r:sshd_key_t:s0
Access: 2021-11-08 13:25:26.107417581 -0500
Modify: 2021-08-12 13:26:25.409353797 -0400
Change: 2021-08-12 13:26:25.421353798 -0400
Birth: -
```

Remediation:

Run the following commands to set permissions, ownership, and group on the private SSH host key files:

```
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec chmod u-x,g-wx,o-rwx {} \;

# find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec chown
root:ssh_keys
OR
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec chown root:root {}
\;
```

Default Value:

Access: (0640/-rw-r-----) Uid: (0/ root) Gid: ({gid}/ssh_keys)

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204597
Rule ID: SV-204597r603261_rule
STIG ID: RHEL-07-040420
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

5.3.5 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:

```
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec stat {} \;
```

Example Output:

```
File: '/etc/ssh/ssh_host_rsa_key.pub'
Size: 382          Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d Inode: 8631758      Links: 1
Access: (0644/-rw-r--r--)  Uid: (   0/   root)   Gid: (   0/   root)
Access: 2018-10-22 18:24:56.861750616 +0000
Modify: 2018-10-22 18:24:56.861750616 +0000
Change: 2018-10-22 18:24:56.881750616 +0000
Birth: -
File: '/etc/ssh/ssh_host_ecdsa_key.pub'
Size: 162          Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d Inode: 8631761      Links: 1
Access: (0644/-rw-r--r--)  Uid: (   0/   root)   Gid: (   0/   root)
Access: 2018-10-22 18:24:56.897750616 +0000
Modify: 2018-10-22 18:24:56.897750616 +0000
Change: 2018-10-22 18:24:56.917750616 +0000
Birth: -
File: '/etc/ssh/ssh_host_ed25519_key.pub'
Size: 82           Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d Inode: 8631763      Links: 1
Access: (0644/-rw-r--r--)  Uid: (   0/   root)   Gid: (   0/   root)
Access: 2018-10-22 18:24:56.945750616 +0000
Modify: 2018-10-22 18:24:56.945750616 +0000
Change: 2018-10-22 18:24:56.961750616 +0000
Birth: -
```

Remediation:

Run the following commands to set permissions and ownership on the SSH host public key files

```
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec chmod u-x,go-  
wx {} \;  
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec chown  
root:root {} \;
```

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204596
Rule ID: SV-204596r603261_rule
STIG ID: RHEL-07-040410
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

5.3.6 Ensure SSH access is limited (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 commands and verify the output:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname)
/etc/hosts | awk '{print $1}')" | grep -Pi
'^\h*(allow|deny) (users|groups) \h+\H+(\h+.*?)?$'

# grep -Pi '^ \h*(allow|deny) (users|groups) \h+\H+(\h+.*?)?$'
/etc/ssh/sshd_config
```

Verify that the output of both commands matches at least one of the following lines:

```
allowusers <userlist>
allowgroups <grouplist>
denyusers <userlist>
denygroups <grouplist>
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set one or more of the parameter as follows:

```
AllowUsers <userlist>
```

OR

```
AllowGroups <grouplist>
```

OR

```
DenyUsers <userlist>
```

OR

```
DenyGroups <grouplist>
```

Default Value:

None

References:

1. SSHD_CONFIG(5)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> 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	4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u> 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.			

5.3.7 Ensure SSH LogLevel is appropriate (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

`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.

`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.

Rationale:

SSH provides several logging levels with varying amounts of verbosity. `DEBUG` is specifically **not** recommended other than strictly for debugging SSH communications since it provides so much data that it is difficult to identify important security information.

Audit:

Run the following command and verify that output matches `loglevel VERBOSE` or `loglevel INFO`:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep loglevel  
  
loglevel VERBOSE or loglevel INFO
```

Run the following command and verify the output matches:

```
# grep -i 'loglevel' /etc/ssh/sshd_config | grep -Evi '(VERBOSE|INFO)'  
  
Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
LogLevel VERBOSE
```

OR

```
LogLevel INFO
```

Default Value:

LogLevel INFO

References:

1. https://www.ssh.com/ssh/sshd_config/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

5.3.8 Ensure SSH X11 forwarding is disabled (Automated)

Profile Applicability:

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

Description:

The X11Forwarding parameter provides the ability to tunnel X11 traffic through an existing SSH shell session 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.

Impact:

X11 programs on the server will not be able to be forwarded to a ssh-client display.

Audit:

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i x11forwarding
x11forwarding no
```

Run the following command and verify that the output matches:

```
# grep -Ei '^s*x11forwarding\s+yes' /etc/ssh/sshd_config
Nothing is returned
```

Remediation:

Edit the /etc/ssh/sshd_config file to set the parameter as follows:

```
X11Forwarding no
```

Default Value:

X11Forwarding yes

References:

1. SSHD_CONFIG(5)
2. CCI-000366: The organization implements the security configuration settings
3. NIST SP 800-53 :: CM-6 b
4. NIST SP 800-53A :: CM-6.1 (iv)
5. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204622
Rule ID: SV-204622r603849_rule
STIG ID: RHEL-07-040710
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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.3.9 Ensure SSH MaxAuthTries is set to 4 or less (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 output `MaxAuthTries` is 4 or less:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep maxauthtries
maxauthtries 4
```

Run the following command and verify that the output:

```
# grep -Ei '^s*maxauthtries\s+([5-9]|[1-9][0-9]+)' /etc/ssh/sshd_config
Nothing is returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
MaxAuthTries 4
```

Default Value:

`MaxAuthTries 6`

References:

1. SSHD_CONFIG(5)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> 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	16.13 <u>Alert on Account Login Behavior Deviation</u> Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			

5.3.10 Ensure SSH IgnoreRhosts is enabled (Automated)

Profile Applicability:

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

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 and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep ignorerhosts
ignorerhosts yes
```

Run the following command and verify the output:

```
# grep -Ei '^s*ignorerhosts\s+no\b' /etc/ssh/sshd_config
Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
IgnoreRhosts yes
```

Default Value:

`IgnoreRhosts yes`

References:

1. SSHD_CONFIG(5)
2. CCI-000366: The organization implements the security configuration settings
3. NIST SP 800-53 :: CM-6 b
4. NIST SP 800-53A :: CM-6.1 (iv)
5. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204590
Rule ID: SV-204590r603261_rule
STIG ID: RHEL-07-040350
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.3.11 Ensure SSH HostbasedAuthentication is disabled (Automated)

Profile Applicability:

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

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. This option only applies to SSH Protocol Version 2.

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 and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep hostbasedauthentication  
hostbasedauthentication no
```

Run the following command and verify the output matches:

```
# grep -Ei '^s*HostbasedAuthentication\s+yes' /etc/ssh/sshd_config  
Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
HostbasedAuthentication no
```

Default Value:

`HostbasedAuthentication no`

References:

1. SSHD_CONFIG(5)
2. CCI: CCI-000366: The organization implements the security configuration settings.
3. NIST SP 800-53 :: CM-6 b
4. NIST SP 800-53A :: CM-6.1 (iv)
5. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204435
Rule ID: SV-204435r603261_rule
STIG ID: RHEL-07-010470
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	16.3 <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

5.3.12 Ensure SSH root login is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `PermitRootLogin` parameter specifies if the root user can log in using ssh. The default is no.

Rationale:

Disallowing root logins over SSH requires system admins to authenticate using their own individual account, then escalating to root via `sudo`. This in turn limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident

Audit:

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep permitrootlogin  
permitrootlogin no
```

Run the following command and verify the output:

```
# grep -Ei '^s*PermitRootLogin\s+yes' /etc/ssh/sshd_config  
Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitRootLogin no
```

Default Value:

`PermitRootLogin without-password`

References:

1. SSHD_CONFIG(5)
2. CCI-000366: The organization implements the security configuration settings
3. NIST SP 800-53 :: CM-6 b
4. NIST SP 800-53A :: CM-6.1 (iv)
5. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204592
Rule ID: SV-204592r603261_rule
STIG ID: RHEL-07-040370
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> 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	<u>4.3 Ensure the Use of Dedicated Administrative Accounts</u> 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.			

5.3.13 Ensure SSH PermitEmptyPasswords is disabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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 and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep permitemptypasswords
permitemptypasswords no
```

Run the following command and verify the output:

```
# grep -Ei '^s*PermitEmptyPasswords\s+yes' /etc/ssh/sshd_config
Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitEmptyPasswords no
```

Default Value:

`PermitEmptyPasswords no`

References:

1. SSHD_CONFIG(5)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204425
Rule ID: SV-204425r603261_rule
STIG ID: RHEL-07-010300
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>16.3 Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

5.3.14 Ensure SSH 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 a Trojan's programs)

Audit:

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep permituserenvironment  
permituserenvironment no
```

Run the following command and verify the output:

```
# grep -Ei '^s*PermitUserEnvironment\s+yes' /etc/ssh/sshd_config  
Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitUserEnvironment no
```

Default Value:

`PermitUserEnvironment no`

References:

1. SSHD_CONFIG(5)
2. CCI: CCI-000366: The organization implements the security configuration settings.
3. NIST SP 800-53 :: CM-6 b
4. NIST SP 800-53A :: CM-6.1 (iv)
5. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204434
Rule ID: SV-204434r603261_rule
STIG ID: RHEL-07-010460
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

5.3.15 Ensure only strong Ciphers are used (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

This variable limits the ciphers that SSH can use during communication.

Note: Some organizations may have stricter requirements for approved ciphers. Ensure that ciphers used are in compliance with site policy.

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 DES, Triple DES, and Blowfish ciphers, as used in SSH, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, aka a "Sweet32" attack
- The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue
- The passwords used during an SSH session encrypted with RC4 can be recovered by an attacker who is able to capture and replay the session
- 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 plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors

Audit:

Run the following command and verify the output:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -Ei '^\\s*ciphers\\s+([\\^#]+,)?(3des-cbc|aes128-cbc|aes192-cbc|aes256-cbc|arcfour|arcfour128|arcfour256|blowfish-cbc|cast128-cbc|rijndael-cbc@lysator.liu.se)\\b'
```

Nothing should be returned

Run the following command and verify the output:

```
grep -Ei '^\\s*ciphers\\s+([\\^#]+,)?(3des-cbc|aes128-cbc|aes192-cbc|aes256-cbc|arcfour|arcfour128|arcfour256|blowfish-cbc|cast128-cbc|rijndael-cbc@lysator.liu.se)\\b' /etc/ssh/sshd_config
```

Nothing should be returned

Remediation:

Edit the `/etc/ssh/sshd_config` file add/modify the `Ciphers` line to contain a comma separated list of the site approved ciphers

Example:

```
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
```

Default Value:

Ciphers chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-cbc,aes192-cbc,aes256-cbc,blowfish-cbc,cast128-cbc,3des-cbc

References:

1. <https://nvd.nist.gov/vuln/detail/CVE-2016-2183>
2. <https://nvd.nist.gov/vuln/detail/CVE-2015-2808>
3. <https://www.kb.cert.org/vuls/id/565052>
4. <https://www.openssh.com/txt/cbc.adv>
5. <https://nvd.nist.gov/vuln/detail/CVE-2008-5161>
6. <https://nvd.nist.gov/vuln/detail/CVE-2013-4548>
7. <https://www.kb.cert.org/vuls/id/565052>
8. <https://www.openssh.com/txt/cbc.adv>
9. SSHD_CONFIG(5)

Additional Information:

Weak Ciphers:

```
3des-cbc  
aes128-cbc  
aes192-cbc  
aes256-cbc  
arcfour  
arcfour128  
arcfour256  
blowfish-cbc  
cast128-cbc  
rijndael-cbc@lysator.liu.se
```

Ciphers supported by openSSH v7.4p1:

```
3des-cbc  
aes128-cbc  
aes192-cbc  
aes256-cbc  
aes128-ctr  
aes192-ctr  
aes256-ctr  
aes128-gcm@openssh.com  
aes256-gcm@openssh.com  
arcfour  
arcfour128  
arcfour256  
blowfish-cbc  
cast128-cbc  
chacha20-poly1305@openssh.com
```

Ciphers currently FIPS 140-2 approved:

```
aes256-gcm@openssh.com  
aes128-gcm@openssh.com  
aes256-ctr  
aes192-ctr  
aes128-ctr
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> 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> Encrypt all sensitive information in transit.			

5.3.16 Ensure only FIPS 140-2 ciphers are used for SSH (Automated)

Profile Applicability:

- STIG

Description:

The operating system must use a FIPS 140-2 approved cryptographic algorithm for SSH communications.

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.

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:

The only "strong" ciphers currently FIPS 140-2 compliant are: aes256-ctr,aes192-ctr,aes128-ctr

Audit:

Verify the operating system uses mechanisms meeting the requirements of applicable federal laws, Executive orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

Note: If Benchmark recommendation 1.5.7 fails, this is automatically a finding as the system cannot implement FIPS 140-2-approved cryptographic algorithms and hashes.

The location of the `sshd_config` file may vary if a different daemon is in use. The command below utilizes this path `/etc/ssh/sshd_config`.

Inspect the `Ciphers` configuration with the following command:

```
# grep -i ciphers /etc/ssh/sshd_config  
Ciphers aes128-ctr,aes192-ctr,aes256-ctr
```

If any ciphers other than `aes128-ctr`, `aes192-ctr`, or `aes256-ctr` are listed, the `Ciphers` keyword is missing, or the returned line is commented out, refer to the remediation procedure below.

Remediation:

Configure SSH to use FIPS 140-2 approved cryptographic algorithms.

Add the following line (or modify the line to have the required value) to the `/etc/ssh/sshd_config` file (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).

Example: `vim /etc/ssh/sshd_config`

Add, uncomment or update the following line:

```
Ciphers aes128-ctr,aes192-ctr,aes256-ctr
```

The SSH service must be restarted for changes to take effect.

```
# systemctl restart sshd.service
```


References:

1. CCI-000068: The information system implements cryptographic mechanisms to protect the confidentiality of remote access sessions
2. NIST SP 800-53 :: AC-17 (2)
3. NIST SP 800-53A :: AC-17 (2).1
4. NIST SP 800-53 Revision 4 :: AC-17 (2)
5. CCI-000366: The organization implements the security configuration settings
6. NIST SP 800-53 :: CM-6 b
7. NIST SP 800-53A :: CM-6.1 (iv)
8. NIST SP 800-53 Revision 4 :: CM-6 b
9. CCI-000803: The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication
10. NIST SP 800-53 :: IA-7
11. NIST SP 800-53A :: IA-7.1
12. NIST SP 800-53 Revision 4 :: IA-7

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204578
Rule ID: SV-204578r744116_rule
STIG ID: RHEL-07-040110
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> 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> Encrypt all sensitive information in transit.			

5.3.17 Ensure only strong MAC algorithms are used (Automated)

Profile Applicability:

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

Description:

This variable Specifies the available MAC (message authentication code) algorithms. The MAC algorithm is used in protocol version 2 for data integrity protection. Multiple algorithms must be comma-separated.

Note: Some organizations may have stricter requirements for approved MACs. Ensure that MACs used are in compliance with site policy.

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 and verify the output:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -Ei '^\\s*macs\\s+([\\^#]+,)?(hmac-md5|hmac-md5-96|hmac-ripemd160|hmac-sha1|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-etm@openssh\\.com|hmac-sha1-96-etm@openssh\\.com|umac-64-etm@openssh\\.com|umac-128-etm@openssh\\.com)\\b'
```

Nothing should be returned

Run the following command and verify the output:

```
# grep -Ei '^\\s*macs\\s+([\\^#]+,)?(hmac-md5|hmac-md5-96|hmac-ripemd160|hmac-sha1|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-etm@openssh\\.com|hmac-sha1-96-etm@openssh\\.com|umac-64-etm@openssh\\.com|umac-128-etm@openssh\\.com)\\b' /etc/ssh/sshd_config
```

Nothing should be returned

Remediation:

Edit the `/etc/ssh/sshd_config` file and add/modify the MACs line to contain a comma separated list of the site approved MACs

Example:

```
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512,hmac-sha2-256
```

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,hmac-sha1-etm@openssh.com
```

References:

1. More information on SSH downgrade attacks can be found here:
<http://www.mitls.org/pages/attacks/SLOTH>
2. SSHD_CONFIG(5)
3. CCI-001453: The information system implements cryptographic mechanisms to protect the integrity of remote access sessions
4. NIST SP 800-53 :: AC-17 (2)
5. NIST SP 800-53A :: AC-17 (2).1
6. NIST SP 800-53 Revision 4 :: AC-17 (2)

Additional Information:

Weak MAC algorithms:

```
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-sha1
hmac-sha1-96
umac-64@openssh.com
umac-128@openssh.com
hmac-md5-etm@openssh.com
hmac-md5-96-etm@openssh.com
hmac-ripemd160-etm@openssh.com
hmac-sha1-etm@openssh.com
hmac-sha1-96-etm@openssh.com
umac-64-etm@openssh.com
umac-128-etm@openssh.com
```

MAC algorithms supported by openSSH v7.4p1:

```
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-sha1
hmac-sha1-96
hmac-sha2-256
hmac-sha2-512
umac-64@openssh.com
umac-128@openssh.com
hmac-md5-etm@openssh.com
hmac-md5-96-etm@openssh.com
hmac-ripemd160-etm@openssh.com
hmac-sha1-etm@openssh.com
hmac-sha1-96-etm@openssh.com
hmac-sha2-256-etm@openssh.com
hmac-sha2-512-etm@openssh.com
umac-64-etm@openssh.com
umac-128-etm@openssh.com
```

MACs algorithms currently FIPS 140-2 approved:

```
hmac-sha2-512-etm@openssh.com
hmac-sha2-256-etm@openssh.com
hmac-sha2-256
hmac-sha2-512
Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204595
Rule ID: SV-204595r744117_rule
STIG ID: RHEL-07-040400
Severity: CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> 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> Encrypt all sensitive information in transit.			
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.			

5.3.18 Ensure only strong Key Exchange algorithms are used (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

Note: Some organizations may have stricter requirements for approved Key Exchange algorithms. Ensure that Key Exchange algorithms used are in compliance with site policy.

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 and verify the output:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -Ei '^\\s*kexalgorithms\\s+([\\^#]+,)?(diffie-hellman-group1-sha1|diffie-hellman-group14-sha1|diffie-hellman-group-exchange-sha1)\\b'
```

Nothing should be returned

Run the following command and verify the output:

```
# grep -Ei '^\\s*kexalgorithms\\s+([\\^#]+,)?(diffie-hellman-group1-sha1|diffie-hellman-group14-sha1|diffie-hellman-group-exchange-sha1)\\b' /etc/ssh/sshd_config
```

Nothing should be returned

Remediation:

Edit the `/etc/ssh/sshd_config` file add/modify the `KexAlgorithms` line to contain a comma separated list of the site approved key exchange algorithms

Example:

```
KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256
```

Default Value:

```
kexalgorithms curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
```

References:

1. SSHD_CONFIG(5)

Additional Information:

Weak Key Exchange Algorithms:

```
diffie-hellman-group1-sha1  
diffie-hellman-group14-sha1  
diffie-hellman-group-exchange-sha1
```

Key Exchange algorithms supported by OpenSSH 7.4p1:

```
curve25519-sha256  
curve25519-sha256@libssh.org  
diffie-hellman-group1-sha1  
diffie-hellman-group14-sha1  
diffie-hellman-group-exchange-sha1  
diffie-hellman-group-exchange-sha256  
ecdh-sha2-nistp256  
ecdh-sha2-nistp384  
ecdh-sha2-nistp521
```

Key Exchange algorithms currently FIPS 140-2 approved:

```
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
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

5.3.19 Ensure SSH Idle Timeout Interval is configured (Automated)

Profile Applicability:

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

Description:

The two options `ClientAliveInterval` and `ClientAliveCountMax` control the timeout of ssh sessions.

- `ClientAliveInterval` sets 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 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 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. The default value is 3.
 - The client alive messages are sent through the encrypted channel
 - Setting `ClientAliveCountMax` to 0 disables connection termination

Example: 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

Rationale:

Having no timeout value associated with a connection could allow an unauthorized user access to another user's ssh session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value reduces this risk.

- The recommended `ClientAliveInterval` setting is no greater than 600 seconds (10 minutes)
- The recommended `ClientAliveCountMax` setting is 0
- At the 15 minute interval, if the ssh session is inactive, the session will be terminated.

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 commands and verify `ClientAliveInterval` is between 1 and 900:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep clientaliveinterval  
clientaliveinterval 600
```

Run the following command and verify `ClientAliveCountMax` is 0:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep clientalivecountmax  
clientalivecountmax 0
```

Run the following commands and verify the output:

```
# grep -Ei '^\s*ClientAliveInterval\s+(0|9[0-9][1-9]|[1-9][0-9][0-9][0-9]+|1[6-9]m|[2-9][0-9]m|[1-9][0-9][0-9]+m)\b' /etc/ssh/sshd_config  
Nothing should be returned  
  
# grep -Ei '^\s*ClientAliveCountMax\s+([1-9]|[1-9][0-9]+)\b' /etc/ssh/sshd_config  
Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameters according to site policy. This should include `ClientAliveInterval` between 1 and 600 and `ClientAliveCountMax` of 0:

```
ClientAliveInterval 600  
ClientAliveCountMax 0
```

Default Value:

`ClientAliveInterval` 0

`ClientAliveCountMax` 3

References:

1. https://man.openbsd.org/sshd_config
2. CCI-001133: The information system terminates the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity
3. NIST SP 800-53 :: SC-10
4. NIST SP 800-53A :: SC-10.1 (ii)
5. NIST SP 800-53 Revision 4 :: SC-10
6. CCI-002361: The information system automatically terminates a user session after organization-defined conditions or trigger events requiring session disconnect
7. NIST SP 800-53 Revision 4 :: AC-12

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204587
Rule ID: SV-204587r603261_rule
STIG ID: RHEL-07-040320
Severity: CAT II

Vul ID: V-204589
Rule ID: SV-204589r603261_rule
STIG ID: RHEL-07-040340
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process 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	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.			

5.3.20 Ensure SSH LoginGraceTime is set to one minute or less (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 or 1m:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep logingracetime  
logingracetime 60
```

Run the following command and verify the output:

```
# grep -Ei '^s*LoginGraceTime\s+(0|6[1-9]|[7-9][0-9]|[1-9][0-9][0-9]+|^[^1]m)' /etc/ssh/sshd_config  
Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
LoginGraceTime 60
```

Default Value:

LoginGraceTime 2m

References:

1. SSHD_CONFIG(5)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

5.3.21 Ensure SSH warning 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 and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep banner  
banner /etc/issue.net
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Banner /etc/issue.net
```

References:

1. SSHD_CONFIG(5)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

5.3.22 Ensure SSH PAM is enabled (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

UsePAM Enables the Pluggable Authentication Module interface. If set to “yes” this will enable PAM authentication using ChallengeResponseAuthentication and PasswordAuthentication 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

Impact:

If UsePAM is enabled, you will not be able to run sshd(5) as a non-root user.

Audit:

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i usepam  
usepam yes
```

Run the following command and verify the output:

```
# grep -Ei '^s*UsePAM\s+no' /etc/ssh/sshd_config  
Nothing should be returned
```

Remediation:

Edit the /etc/ssh/sshd_config file to set the parameter as follows:

```
UsePAM yes
```


Default Value:

usePAM yes

References:

1. SSHD_CONFIG(5)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

5.3.23 Ensure SSH AllowTcpForwarding is disabled (Automated)

Profile Applicability:

- Level 2 - Server
- Level 2 - Workstation

Description:

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:

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 that employ mainframe systems as their application backends. In those 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 and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i allowtcpforwarding  
allowtcpforwarding no
```

Run the following command and verify the output:

```
# grep -Ei '^s*AllowTcpForwarding\s+yes' /etc/ssh/sshd_config  
Nothing should be returned
```

Remediation:

Edit the /etc/ssh/sshd_config file to set the parameter as follows:

```
AllowTcpForwarding no
```

Default Value:

AllowTcpForwarding yes

References:

1. <https://www.ssh.com/ssh/tunneling/example>
2. SSHD_CONFIG(5)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			
v7	<u>13.5 Monitor and Detect Any Unauthorized Use of Encryption</u> Monitor all traffic leaving the organization and detect any unauthorized use of encryption.			

5.3.24 Ensure SSH 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 and verify that output `MaxStartups` is `10:30:60` or more restrictive:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i maxstartups  
  
maxstartups 10:30:60
```

Run the following command and verify the output:

```
# grep -Ei '^\s*maxstartups\s+(((1[0-9]|[0-9][0-9]+):([0-9]+):([0-9]+))|((([0-9]+):(3[0-9]|[4-9][0-9]|[1-9][0-9][0-9]+):([0-9]+))|((([0-9]+):([0-9]+):(6[0-9]|[7-9][0-9]|[1-9][0-9][0-9]+)))' /etc/ssh/sshd_config  
  
Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
maxstartups 10:30:60
```

Default Value:

`MaxStartups 10:30:100`

References:

1. SSHD_CONFIG(5)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

5.3.25 Ensure SSH MaxSessions is limited (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `MaxSessions` parameter Specifies the maximum number of open sessions permitted per network 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 output `MaxSessions` is 10 or less:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i maxsessions  
maxsessions 10
```

Run the following command and verify the output:

```
grep -Ei '^s*MaxSessions\s+(1[1-9]|[2-9][0-9]|[1-9][0-9][0-9]+) '  
/etc/ssh/sshd_config  
Nothing should be returned
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
MaxSessions 10
```

Default Value:

`MaxSessions 10`

References:

1. SSHD_CONFIG(5)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

5.3.26 Ensure RSA rhosts authentication is not allowed (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that the SSH daemon does not allow authentication using RSA rhosts authentication.

Rationale:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Audit:

Check the version of the operating system with the following command:

```
# cat /etc/redhat-release
```

If the release is 7.4 or newer this requirement is Not Applicable. If it is an older release follow the audit below.

Verify the SSH daemon does not allow authentication using RSA rhosts authentication. To determine how the SSH daemon's `RhostsRSAAuthentication` option is set, run the following command:

```
# grep RhostsRSAAuthentication /etc/ssh/sshd_config  
RhostsRSAAuthentication no
```

If the value is returned as `yes`, the returned line is commented out, or no output is returned, refer to the remediation procedure below.

Remediation:

Configure the SSH daemon to not allow authentication using RSA rhosts authentication.
Add the following line in `/etc/ssh/sshd_config`, or uncomment the line and set the value to no:

Example: `vim /etc/ssh/sshd_config`

Add, uncomment or update the following line:

```
RhostsRSAAuthentication no
```

The SSH service must be restarted for changes to take effect.

```
# systemctl restart sshd.service
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide  
Version 3, Release: 4 Benchmark Date: 23 Jul 2021
```

```
Vul ID: V-204588  
Rule ID: SV-204588r603261_rule  
STIG ID: RHEL-07-040330  
Severity: CAT II
```

5.3.27 Ensure 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.

Check that `PrintLastLog` keyword in the `sshd` daemon configuration file is used and set to `yes` with the following command:

```
# grep -i printlastlog /etc/ssh/sshd_config  
PrintLastLog yes
```

If the `PrintLastLog` keyword is set to `no`, is missing, or is commented out, refer to the remediation procedure below.

Remediation:

Configure SSH to provide users with feedback on when account accesses last occurred by setting the required configuration options in `/etc/pam.d/sshd` 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:

Example: `vim /etc/ssh/sshd_config`

Add, uncomment or update the following line:

```
PrintLastLog yes
```

The SSH service must be restarted for changes to `sshd_config` to take effect.

```
# systemctl restart sshd.service
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204591
Rule ID: SV-204591r603261_rule
STIG ID: RHEL-07-040360
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

5.3.28 Ensure SSH IgnoreUserKnownHosts is enabled (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that the SSH daemon does not allow authentication using known hosts authentication.

Rationale:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Audit:

Verify the SSH daemon does not allow authentication using known hosts authentication. To determine how the SSH daemon's `IgnoreUserKnownHosts` option is set, run the following command:

```
# grep -i IgnoreUserKnownHosts /etc/ssh/sshd_config  
IgnoreUserKnownHosts yes
```

If the value is returned as `no`, the returned line is commented out, or no output is returned, refer to the remediation procedure below.

Remediation:

Configure the SSH daemon to not allow authentication using known hosts authentication. Add the following line in `/etc/ssh/sshd_config`, or uncomment the line and set the value to `yes`:

Example: `vim /etc/ssh/sshd_config`

Add, uncomment, or update the following line.

```
IgnoreUserKnownHosts yes
```

The SSH service must be restarted for changes to take effect.

```
# systemctl restart sshd.service
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204593
Rule ID: SV-204593r603261_rule
STIG ID: RHEL-07-040380
Severity: CAT II

5.3.29 Ensure SSH Protocol is set to 2 (Automated)

Profile Applicability:

- STIG

Description:

The Linux operating system must be configured so that the SSH daemon is configured to only use the SSHv2 protocol.

Rationale:

SSHv1 is an insecure implementation of the SSH protocol and has many well-known vulnerability exploits. Exploits of the SSH daemon could provide immediate root access to the system.

Satisfies: SRG-OS-000074-GPOS-00042, SRG-OS-000480-GPOS-00227

Audit:

Check the version of the operating system with the following command:

```
# cat /etc/redhat-release
```

Note: If the release is 7.4 or newer this requirement is Not Applicable.

Verify the SSH daemon is configured to only use the SSHv2 protocol.

Check that the SSH daemon is configured to only use the SSHv2 protocol with the following command:

```
# grep -i protocol /etc/ssh/sshd_config  
  
Protocol 2  
#Protocol 1,2
```

If any protocol line other than "Protocol 2" is uncommented, this is a finding

Remediation:

Remove all Protocol lines that reference version "1" in "/etc/ssh/sshd_config" (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). The "Protocol" line must be as follows:

```
Protocol 2
```

The SSH service must be restarted for changes to take effect

References:

1. CCI-000197: The information system, for password-based authentication, transmits only encrypted representations of passwords
2. NIST SP 800-53 :: IA-5 (1) (c)
3. NIST SP 800-53A :: IA-5 (1).1 (v)
4. NIST SP 800-53 Revision 4 :: IA-5 (1) (c)
5. CCI-000366: The organization implements the security configuration settings
6. NIST SP 800-53 :: CM-6 b
7. NIST SP 800-53A :: CM-6.1 (iv)
8. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

This command no longer exists in newer versions of SSH. This check is still being included for systems that may be running an older version of SSH. As of openSSH version 7.4 this parameter will not cause an issue when included.

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204594
Rule ID: SV-204594r603261_rule
STIG ID: RHEL-07-040390
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.5 <u>Use Multifactor Authentication For All Administrative Access</u> Use multi-factor authentication and encrypted channels for all administrative account access.			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			
v6	3.4 <u>Use Only Secure Channels For Remote System Administration</u> Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.			

5.3.30 Ensure SSH does not permit GSSAPI (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that the SSH daemon does not permit Generic Security Service Application Program Interface (GSSAPI) authentication unless needed.

Rationale:

GSSAPI authentication is used to provide additional authentication mechanisms to applications. Allowing GSSAPI authentication through SSH exposes the system's GSSAPI to remote hosts, increasing the attack surface of the system. GSSAPI authentication must be disabled unless needed.

Audit:

Verify the SSH daemon does not permit GSSAPI authentication unless approved.
Check that the SSH daemon does not permit GSSAPI authentication with the following command:

```
# grep -i gssapiauth /etc/ssh/sshd config
GSSAPIAuthentication no
```

If the `GSSAPIAuthentication` keyword is missing, is set to `yes` and is not documented with the Authorizing Official, or the returned line is commented out, refer to the remediation procedure below.

Remediation:

Uncomment the `GSSAPIAuthentication` keyword in `/etc/ssh/sshd_config` (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) and set the value to `no`:

Example: `vim /etc/ssh/sshd_config`

Add, uncomment or update the following line:

```
GSSAPIAuthentication no
```

The SSH service must be restarted for changes to take effect.

```
# systemctl restart sshd.service
```

If GSSAPI authentication is required, it must be documented, to include the location of the configuration file.

References:

1. CCI-000318: The organization audits and reviews activities associated with configuration controlled changes to the system
2. NIST SP 800-53 :: CM-3 e
3. NIST SP 800-53A :: CM-3.1 (v)
4. NIST SP 800-53 Revision 4 :: CM-3 f
5. CCI-000368: The organization documents any deviations from the established configuration settings for organization-defined information system components based on organization-defined operational requirements
6. NIST SP 800-53 :: CM-6 c
7. NIST SP 800-53A :: CM-6.1 (v)
8. NIST SP 800-53 Revision 4 :: CM-6 c
9. CCI-001812: The information system prohibits user installation of software without explicit privileged status
10. NIST SP 800-53 Revision 4 :: CM-11 (2)
11. CCI-001813: The information system enforces access restrictions
12. NIST SP 800-53 Revision 4 :: CM-5 (1)
13. CCI-001814: The Information system supports auditing of the enforcement actions
14. NIST SP 800-53 Revision 4 :: CM-5 (1)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204598
Rule ID: SV-204598r603261_rule
STIG ID: RHEL-07-040430
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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.3.31 Ensure SSH does not permit Kerberos authentication (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that the SSH daemon does not permit Kerberos authentication unless needed.

Rationale:

Kerberos authentication for SSH is often implemented using Generic Security Service Application Program Interface (GSSAPI). If Kerberos is enabled through SSH, the SSH daemon provides a means of access to the system's Kerberos implementation. Vulnerabilities in the system's Kerberos implementation may then be subject to exploitation. To reduce the attack surface of the system, the Kerberos authentication mechanism within SSH must be disabled for systems not using this capability.

Audit:

Verify the SSH daemon does not permit Kerberos to authenticate passwords unless approved.

Check that the SSH daemon does not permit Kerberos to authenticate passwords with the following command:

```
# grep -i kerberosauth /etc/ssh/sshd_config  
KerberosAuthentication no
```

If the `KerberosAuthentication` keyword is missing, or is set to `yes` and is not documented with the Authorizing Official, or the returned line is commented out, refer to the remediation procedure below.

Remediation:

Uncomment the `KerberosAuthentication` keyword in `/etc/ssh/sshd_config` (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) and set the value to `no`:

Example: `vim /etc/ssh/sshd_config`

Add, uncomment or update the following line:

```
KerberosAuthentication no
```

The SSH service must be restarted for changes to take effect.

```
# systemctl restart sshd.service
```

If Kerberos authentication is required, it must be documented, to include the location of the configuration file.

References:

1. CCI-000318: The organization audits and reviews activities associated with configuration controlled changes to the system
2. NIST SP 800-53 :: CM-3 e
3. NIST SP 800-53A :: CM-3.1 (v)
4. NIST SP 800-53 Revision 4 :: CM-3 f
5. CCI-000368: The organization documents any deviations from the established configuration settings for organization-defined information system components based on organization-defined operational requirements
6. NIST SP 800-53 :: CM-6 c
7. NIST SP 800-53A :: CM-6.1 (v)
8. NIST SP 800-53 Revision 4 :: CM-6 c
9. CCI-001812: The information system prohibits user installation of software without explicit privileged status
10. NIST SP 800-53 Revision 4 :: CM-11 (2)
11. CCI-001813: The information system enforces access restrictions
12. NIST SP 800-53 Revision 4 :: CM-5 (1)
13. CCI-001814: The Information system supports auditing of the enforcement actions
14. NIST SP 800-53 Revision 4 :: CM-5 (1)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204599
Rule ID: SV-204599r603261_rule
STIG ID: RHEL-07-040440
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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.3.32 Ensure SSH performs checks of home directory configuration files (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that the SSH daemon performs 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:

Verify the SSH daemon performs strict mode checking of home directory configuration files.

The location of the `sshd_config` file may vary if a different daemon is in use.

Inspect the `sshd_config` file with the following command:

```
# grep -i strictmodes /etc/ssh/sshd_config
StrictModes yes
```

If `StrictModes` is set to `no`, is missing, or the returned line is commented out, refer to the remediation procedure below.

Remediation:

Uncomment the `StrictModes` keyword in `/etc/ssh/sshd_config` (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) and set the value to `yes`:

Example: `vim /etc/ssh/sshd_config`

Add, uncomment or update the following line:

```
StrictModes yes
```

The SSH service must be restarted for changes to take effect.

```
# systemctl restart sshd.service
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204600
Rule ID: SV-204600r603261_rule
STIG ID: RHEL-07-040450
Severity: CAT II

5.3.33 Ensure SSH uses privilege separation (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that the SSH daemon uses privilege separation.

Rationale:

SSH daemon privilege separation causes the SSH process to drop root privileges when not needed, which would decrease the impact of software vulnerabilities in the unprivileged section.

Audit:

Verify the SSH daemon performs privilege separation.

Check that the SSH daemon performs privilege separation with the following command:

```
# grep -i usepriv /etc/ssh/sshd_config  
UsePrivilegeSeparation sandbox
```

If the `UsePrivilegeSeparation` keyword is set to `no`, is missing, or the returned line is commented out, refer to the remediation procedure below.

Remediation:

Uncomment the `UsePrivilegeSeparation` keyword in `/etc/ssh/sshd_config` (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) and set the value to `sandbox` or `yes`:

Example: `vim /etc/ssh/sshd_config`

Add, uncomment or update the following line:

```
UsePrivilegeSeparation sandbox
```

The SSH service must be restarted for changes to take effect.

```
# systemctl restart sshd.service
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204601
Rule ID: SV-204601r603261_rule
STIG ID: RHEL-07-040460
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> 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	8.3 <u>Enable Operating System Anti-Exploitation Features/Deploy Anti-Exploit Technologies</u> 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.			

5.3.34 Ensure SSH compressions setting is delayed (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that the SSH daemon does not allow compression or only allows compression after successful authentication.

Rationale:

If compression is allowed in an SSH connection prior to authentication, vulnerabilities in the compression software could result in compromise of the system from an unauthenticated connection, potentially with root privileges.

Audit:

Verify the SSH daemon performs compression after a user successfully authenticates. Check that the SSH daemon performs compression after a user successfully authenticates with the following command:

```
# grep -i compression /etc/ssh/sshd_config  
Compression delayed
```

If the `Compression` keyword is set to `yes`, is missing, or the returned line is commented out, refer to the remediation procedure below.

Remediation:

Uncomment the `Compression` keyword in `/etc/ssh/sshd_config` (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) on the system and set the value to `delayed` or `no`:

Example: `vim /etc/ssh/sshd_config`

Add, uncomment or update the following line:

```
Compression no
```

The SSH service must be restarted for changes to take effect.

```
# systemctl restart sshd.service
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204602
Rule ID: SV-204602r603261_rule
STIG ID: RHEL-07-040470
Severity: CAT II

5.3.35 Ensure SSH X11UseLocalhost is enabled (Automated)

Profile Applicability:

- STIG

Description:

The Linux operating system 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. Check the SSH X11UseLocalhost setting with the following command:

```
# grep -i x11uselocalhost /etc/ssh/sshd_config  
X11UseLocalhost yes
```

If the "X11UseLocalhost" keyword is set to "no", is missing, or is commented out, this is a finding.

Remediation:

Configure the SSH daemon to prevent remote hosts from connecting to the proxy display. Edit the "/etc/ssh/sshd_config" file to uncomment or add the line for the "X11UseLocalhost" keyword and set its value to "yes" (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):

```
X11UseLocalhost yes
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-233307
Rule ID: SV-233307r603301_rule
STIG ID: RHEL-07-040711
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> 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> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5.3.36 Ensure no ".shosts" files exist on the system (Manual)

Profile Applicability:

- STIG

Description:

The operating system must not contain .shosts files.

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 system.

Check the system for the existence of these files with the following command:

```
# find / -name '*.shosts'
```

If any .shosts files are found on the system, refer to the remediation procedure below.

Remediation:

Remove any found .shosts files from the system.

Refer to the list found in the Audit section and apply the path to the file in the example below:

```
# rm /[path]/[to]/[file]/.shosts
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204606
Rule ID: SV-204606r603261_rule
STIG ID: RHEL-07-040540
Severity: CAT I

5.3.37 Ensure no "shosts.equiv" files exist on the system (Manual)

Profile Applicability:

- STIG

Description:

The operating system must not contain shosts.equiv files.

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 system.

Check the system for the existence of these files with the following command:

```
# find / -name shosts.equiv
```

If any `shosts.equiv` files are found on the system, refer to the remediation below.

Remediation:

Remove any found `shosts.equiv` files from the system.

Refer to the list found in the Audit section and apply the path to the file in the example below:

```
# rm /[path]/[to]/[file]/shosts.equiv
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204607
Rule ID: SV-204607r603261_rule
STIG ID: RHEL-07-040550
Severity: CAT I

5.4 Configure PAM

PAM (Pluggable Authentication Modules) 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.

5.4.1 Ensure password creation requirements are configured (Automated)

Profile Applicability:

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

Description:

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. The following are definitions of the `pam_pwquality.so` options.

The following options are set in the `/etc/security/pwquality.conf` file:

Password Length:

- `minlen = 14` - password must be 14 characters or more

Password complexity:

- `minclass = 4` - The minimum number of required classes of characters for the new password (digits, uppercase, lowercase, others)
OR
- `dcredit = -1` - provide at least one digit
- `ucredit = -1` - provide at least one uppercase character
- `ocredit = -1` - provide at least one special character
- `lcredit = -1` - provide at least one lowercase character

The following is set in the `/etc/pam.d/password-auth` and `/etc/pam.d/system-auth` files

- `try_first_pass` - retrieve the password from a previous stacked PAM module. If not available, then prompt the user for a password.
- `retry=3` - Allow 3 tries before sending back a failure.

The settings shown above are one possible policy. Alter these values to conform to your own organization's password policies.

Notes:

- *Settings in `/etc/security/pwquality.conf` must use spaces around the `=` symbol.*
- *Additional modules options may be set in the `/etc/pam.d/password-auth` and `/etc/pam.d/system-auth` files*

Rationale:

Strong passwords and limited attempts before locking an account protect systems from being hacked through brute force methods.

Audit:

Verify password creation requirements conform to organization policy.

Run the following command to verify the minimum password length is 14 or more characters.

```
# grep '^s*minlen\s*' /etc/security/pwquality.conf
minlen = 14
```

Run one of the following commands to verify the required password complexity:

```
# grep '^s*minclass\s*' /etc/security/pwquality.conf
minclass = 4
```

OR

```
# grep -E '^s*[duol]credit\s*' /etc/security/pwquality.conf
dcredit = -1
ucredit = -1
lcredit = -1
ocredit = -1
```

Run the following commands to verify the files: /etc/pam.d/password-auth and /etc/pam.d/system-auth include try_first_pass and retry=3 on the password requisite pam_pwquality.so line.

```
# grep -P
'^s*password\s+(?:requisite|required)\s+pam_pwquality\.so\s+(?:\S+\s+)*(?!2
)(retry=[1-3]|try_first_pass)\s+(?:\S+\s+)*(?!1)(retry=[1-
3]|try_first_pass)\s*(?:\s+\S+\s+)*(?:\s+#.*)?$' /etc/pam.d/password-auth

password      requisite      pam_pwquality.so try_first_pass retry=3
# grep -P
'^s*password\s+(?:requisite|required)\s+pam_pwquality\.so\s+(?:\S+\s+)*(?!2
)(retry=[1-3]|try_first_pass)\s+(?:\S+\s+)*(?!1)(retry=[1-
3]|try_first_pass)\s*(?:\s+\S+\s+)*(?:\s+#.*)?$' /etc/pam.d/system-auth

password      requisite      pam_pwquality.so try_first_pass retry=3
```

Remediation:

Edit the file `/etc/security/pwquality.conf` and add or modify the following line for password length to conform to site policy

```
minlen = 14
```

Edit the file `/etc/security/pwquality.conf` and add or modify the following line for password complexity to conform to site policy

```
minclass = 4
```

OR

```
dcredit = -1  
ucredit = -1  
ocredit = -1  
lcredit = -1
```

Edit the `/etc/pam.d/password-auth` and `/etc/pam.d/system-auth` files to include the appropriate options for `pam_pwquality.so` and to conform to site policy:

```
password requisite pam_pwquality.so try_first_pass retry=3
```

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204406
Rule ID: SV-204406r603261_rule
STIG ID: RHEL-07-010119
Severity: CAT II

Vul ID: V-204407
Rule ID: SV-204407r603261_rule
STIG ID: RHEL-07-010120
Severity: CAT II

Vul ID: V-204408
Rule ID: SV-204408r603261_rule
STIG ID: RHEL-07-010130
Severity: CAT II

Vul ID: V-204409
Rule ID: SV-204409r603261_rule
STIG ID: RHEL-07-010140
Severity: CAT II

Vul ID: V-204410
Rule ID: SV-204410r603261_rule
STIG ID: RHEL-07-010150

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> 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	4.4 <u>Use Unique Passwords</u> 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 Ensure logout for failed password attempts is configured (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

Lock out users after *n* unsuccessful consecutive login attempts.

These settings are commonly configured with the `pam_faillock.so` module. Some environments may continue using the `pam_tally2.so` module, where this older method may simplify automation in mixed environments.

Set the logout number in `deny=` to the policy in effect at your site.

`unlock_time=_n_` is the number of seconds the account remains locked after the number of attempts configured in `deny=_n_` has been met.

Notes:

- *Additional module options may be set, recommendation only covers those listed here.*
- *When modifying authentication configuration using the `authconfig` utility, the `system-auth` and `password-auth` files are overwritten with the settings from the `authconfig` utility. This can be avoided by creating symbolic links in place of the configuration files, which `authconfig` recognizes and does not overwrite. These symbolic links are the default for Fedora 19 derived distributions.*
- *Use of the "audit" keyword may log credentials in the case of user error during authentication. This risk should be evaluated in the context of the site policies of your organization.*
- *If a user has been locked out because they have reached the maximum consecutive failure count defined by `deny=` in the `pam_faillock.so` or the `pam_tally2.so` module, the user can be unlocked by issuing following commands. This command sets the failed count to 0, effectively unlocking the user.*
 - *If `pam_faillock.so` is used:*

```
# faillock --user <username> --reset
```
 - *If `pam_tally2.so` is used:*

```
# pam_tally2 -u <username> --reset
```


Rationale:

Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Audit:

Verify password lockouts are configured. Ensure that the `deny=_n_` follows local site policy. This should not exceed `deny=5`.

If `pam_faillock.so` is used:

Run the following commands:

```
# grep -E '^\\s*auth\\s+\\S+\\s+pam_(faillock|unix)\\.so' /etc/pam.d/system-auth
/etc/pam.d/password-auth
```

Verify the output includes the following lines:

```
/etc/pam.d/system-auth:auth          required          pam_faillock.so preauth
silent audit deny=5 unlock_time=900
/etc/pam.d/system-auth:auth          sufficient        pam_unix.so nullok
try_first_pass
/etc/pam.d/system-auth:auth          [default=die] pam_faillock.so authfail
audit deny=5 unlock_time=900
/etc/pam.d/password-auth:auth        required          pam_faillock.so preauth
silent audit deny=5 unlock_time=900
/etc/pam.d/password-auth:auth        sufficient        pam_unix.so nullok
try_first_pass
/etc/pam.d/password-auth:auth        [default=die] pam_faillock.so authfail
audit deny=5 unlock_time=900
# grep -E '^\\s*account\\s+required\\s+pam_faillock.so\\s*' /etc/pam.d/system-
auth /etc/pam.d/password-auth
```

Verify the output includes the following lines:

```
/etc/pam.d/system-auth:account        required          pam_faillock.so
/etc/pam.d/password-auth:account      required          pam_faillock.so
```

OR

If `pam_tally2.so` is used:

Run the following commands:

```
# grep -E '^\\s*auth\\s+\\S+\\s+pam_(tally2|unix)\\.so' /etc/pam.d/system-auth
/etc/pam.d/password-auth
```

Verify the output includes the following lines:

```

/etc/pam.d/system-auth:auth      required      pam_tally2.so deny=5
onerr=fail unlock_time=900
/etc/pam.d/system-auth:auth      sufficient    pam_unix.so nullok
try_first_pass
/etc/pam.d/password-auth:auth    required      pam_tally2.so deny=5
onerr=fail unlock_time=900
/etc/pam.d/password-auth:auth    sufficient    pam_unix.so nullok
try_first_pass
# grep -E '^s*account\s+required\s+pam_tally2.so\s*' /etc/pam.d/system-auth
/etc/pam.d/password-auth

```

Verify the output includes the following lines:

```

/etc/pam.d/system-auth:account    required      pam_tally2.so
/etc/pam.d/password-auth:account required      pam_tally2.so

```

Remediation:

Edit the files `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth` and add the following lines:

Modify the `deny=` and `unlock_time=` parameters to conform to local site policy, Not to be greater than `deny=5`

To use `pam_faillock.so` module, add the following lines to the `auth` section:

```

auth      required      pam_faillock.so preauth silent audit deny=5
unlock_time=900
auth      [default=die] pam_faillock.so authfail audit deny=5
unlock_time=900

```

The `auth` sections should look similar to the following example:

Note: The ordering on the lines in the `auth` section is important. The `preauth` line needs to below the line `auth required pam_env.so` and above all password validation lines. The `authfail` line needs to be after all password validation lines such as `pam_sss.so`. Incorrect order can cause you to be locked out of the system

Example:

```

auth      required      pam_env.so
auth      required      pam_faillock.so preauth silent audit deny=5
unlock_time=900 # <- Under "auth required pam_env.so"
auth      sufficient    pam_unix.so nullok try_first_pass
auth      [default=die] pam_faillock.so authfail audit deny=5
unlock_time=900 # <- Last auth line before "auth requisite
pam_succeed_if.so"
auth      requisite      pam_succeed_if.so uid >= 1000 quiet_success
auth      required      pam_deny.so

```

Add the following line to the `account` section:

account	required	pam_faillock.so

Example:

account	required	pam_faillock.so
account	required	pam_unix.so
account	sufficient	pam_localuser.so
account	sufficient	pam_pam_succeed_if.so uid < 1000 quiet
account	required	pam_permit.so

OR

To use the `pam_tally2.so` module, add the following line to the `auth` section:

auth	required	pam_tally2.so deny=5 onerr=fail unlock_time=900

The `auth` sections should look similar to the following example:

Note: The ordering on the lines in the `auth` section is important. the additional line needs to below the line `auth required pam_env.so` and above all password validation lines.

Example:

auth	required	pam_env.so
auth	required	pam_tally2.so deny=5 onerr=fail unlock_time=900 #
<- Under "auth required pam_env.so"		
auth	sufficient	pam_unix.so nullok try_first_pass
auth	requisite	pam_succeed_if.so uid >= 1000 quiet_success
auth	required	pam_deny.so

Add the following line to the `account` section:

account	required	pam_tally2.so

Example:

account	required	pam_tally2.so
account	required	pam_unix.so
account	sufficient	pam_localuser.so
account	sufficient	pam_pam_succeed_if.so uid < 1000 quiet
account	required	pam_permit.so

References:

1. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>16.7 Establish Process for Revoking Access</u> 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.			

5.4.3 Ensure password hashing algorithm is SHA-512 (Automated)

Profile Applicability:

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

Description:

The commands below change password encryption from md5 to sha512 (a much stronger hashing algorithm). All existing accounts will need to perform a password change to upgrade the stored hashes to the new algorithm.

Note:

- *These changes only apply to accounts configured on the local system.*
- *Additional module options may be set, recommendation only covers those listed here.*

Rationale:

The SHA-512 algorithm provides much stronger hashing than MD5, thus providing additional protection to the system by increasing the level of effort for an attacker to successfully determine passwords.

Audit:

Run the following command to verify the sha512 option is included:

```
# grep -P
'^\h*password\h+(sufficient|required)\h+pam_unix\.so\h+([\#\n\r]+)?
sha512(\h+.)?$' /etc/pam.d/system-auth /etc/pam.d/password-auth

/etc/pam.d/system-auth:password      sufficient      pam_unix.so sha512 shadow
nullok try_first_pass use_authok
/etc/pam.d/password-auth:password    sufficient      pam_unix.so sha512 shadow
nullok try_first_pass use_authok
```

Remediation:

Edit the `/etc/pam.d/password-auth` and `/etc/pam.d/system-auth` files to include sha512 option and remove the md5 option for pam_unix.so:

```
password sufficient pam_unix.so sha512
```

Note:

- Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems.
- If it is determined that the password algorithm being used is not SHA-512, once it is changed, it is recommended that all user ID's be immediately expired and forced to change their passwords on next login, In accordance with local site policies.
- To accomplish this, the following command can be used.
 - This command intentionally does not effect the root account. **The root account's password will also need to be changed.**

```
# awk -F: ' ( $3<"$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)" && $1 !~  
/^(nfs)?nobody$/ && $1 != "root" ) { print $1 }' /etc/passwd | xargs -n 1  
chage -d 0
```

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204415
Rule ID: SV-204415r603261_rule
STIG ID: RHEL-07-010200
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> 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	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.			

5.4.4 Ensure password reuse is limited (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.

Note: Additional module options may be set, recommendation only covers those listed here.

Rationale:

Forcing users not to reuse their past 5 passwords make it less likely that an attacker will be able to guess the password.

Audit:

Verify remembered password history follows local site policy, not to be less than 5.

If `pam_pwhistory.so` is used:

Run the following command:

```
# grep -P
'^\s*password\s+(requisite|required)\s+pam_pwhistory\.so\s+([\^#]+\s+)*remeber=([5-9]|[1-9][0-9]+)\b' /etc/pam.d/system-auth /etc/pam.d/password-auth

/etc/pam.d/system-auth:password      required      pam_pwhistory.so remember=5
/etc/pam.d/password-auth:password    required      pam_pwhistory.so
remember=5
```

OR *If `pam_unix.so` is used:*

Run the following command:

```
# grep -P
'^\s*password\s+(sufficient|required)\s+pam_unix\.so\s+([\^#]+\s+)*remember=([5-9]|[1-9][0-9]+)\b' /etc/pam.d/system-auth /etc/pam.d/password-auth

/etc/pam.d/system-auth:password      sufficient    pam_unix.so remember=5
/etc/pam.d/password-auth:password    sufficient    pam_unix.so remember=5
```

Remediation:

Edit **both** the `/etc/pam.d/password-auth` and `/etc/pam.d/system-auth` files to include the `remember` option and conform to site policy as shown:

Note: Add or modify the line containing the `pam_pwhistory.so` **after the first occurrence of `password requisite`:**

```
password    required    pam_pwhistory.so remember=5
```

Example: (Second line is modified)

```
password    requisite    pam_pwquality.so try_first_pass local_users_only
authtok_type=
password    required    pam_pwhistory.so use_authtok remember=5 retry=3
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass
use_authtok
password    required    pam_deny.so
```

Additional Information:

- This setting only applies to local accounts.
- This option is configured with the `remember=n` module option in `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth`
- This option can be set with either **one** of the two following modules:
 - `pam_pwhistory.so` - This is the newer recommended method included in the remediation section.
 - `pam_unix.so` - This is the *older* method, and is included in the audit to account for legacy configurations.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> 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	16 <u>Account Monitoring and Control</u> Account Monitoring and Control			

5.4.5 Ensure system-auth is used when changing passwords (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that `/etc/pam.d/passwd` implements `/etc/pam.d/system-auth` when changing passwords.

Rationale:

Pluggable authentication modules (PAM) allow for a modular approach to integrating authentication methods. PAM operates in a top-down processing model and if the modules are not listed in the correct order, an important security function could be bypassed if stack entries are not centralized.

Audit:

Verify that `/etc/pam.d/passwd` is configured to use `/etc/pam.d/system-auth` when changing passwords:

```
# cat /etc/pam.d/passwd | grep -i substack | grep -i system-auth  
password substack system-auth
```

If no results are returned, or the line is commented out, refer to the remediation procedure below.

Remediation:

Configure PAM to utilize `/etc/pam.d/system-auth` when changing passwords.

Add the following line to `/etc/pam.d/passwd` (or modify the line to have the required value):

Example: `vim /etc/pam.d/passwd`

Add, uncomment or update the following line:

```
password substack system-auth
```

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204405
Rule ID: SV-204405r603261_rule
STIG ID: RHEL-07-010118
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> 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	4.4 <u>Use Unique Passwords</u> 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.			

5.4.6 Ensure no accounts are configured with blank or null passwords (Automated)

Profile Applicability:

- STIG

Description:

The operating system must not have accounts configured with `blank` or `null` passwords.

Rationale:

If an account has an `blank` password, anyone could log on and run commands with the privileges of that account. Accounts with 'blank' passwords should never be used in operational environments.

Audit:

To verify that null passwords cannot be used, run the following command:

```
# grep nullok /etc/pam.d/system-auth /etc/pam.d/password-auth
```

If this produces any output, it may be possible to log on with accounts with empty passwords.

If null passwords can be used, this is a finding.

Remediation:

If an account is configured for password authentication but does not have an assigned password, it may be possible to log on to the account without authenticating.

Remove any instances of the "nullok" option in `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth` to prevent logons with empty passwords.

Note: Manual changes to the listed files may be overwritten by the "authconfig" program. The "authconfig" program should not be used to update the configurations listed in this requirement.

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204424
Rule ID: SV-204424r603261_rule
STIG ID: RHEL-07-010290
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords 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	4.4 Use Unique Passwords 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.			

5.4.7 Ensure minimum and maximum requirements are set for password changes (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that when passwords are changed a minimum of 8 of the total number of characters must be changed and a minimum of 4 character classes must be changed. The operating system must also be configured so that when passwords are changed the number of repeating consecutive characters must not be more than 3 characters and the number of repeating characters of the same character class must not be more than 4 characters. The operating system must be configured so that passwords are a minimum of 15 characters in length.

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.

Impact:

Consult your documentation for the appropriate PAM file and module. Additional module options may be set, recommendation requirements only cover including `try_first_pass` and `minlen` set to 14 or more. Settings in `/etc/security/pwquality.conf` must use spaces around the `=` symbol.

Audit:

The `difok` option sets the number of characters in a password that must not be present in the old password. The `minclass` option sets the minimum number of required classes of characters for the new password (digits, upper-case, lower-case, others). The `maxrepeat` option sets the maximum number of allowed same consecutive characters in a new password. The `maxclassrepeat` option sets the maximum number of allowed same consecutive characters in the same class in the new password. The `minlen` option sets the minimum number of characters in a new password.

Check for the value of the `difok` option in `/etc/security/pwquality.conf` with the following command:

```
# grep difok /etc/security/pwquality.conf  
difok = 8
```

Check for the value of the `minclass` option in `/etc/security/pwquality.conf` with the following command:

```
# grep minclass /etc/security/pwquality.conf  
minclass = 4
```

Check for the value of the `maxrepeat` option in `/etc/security/pwquality.conf` with the following command:

```
# grep maxrepeat /etc/security/pwquality.conf  
maxrepeat = 3
```

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
```

Check for the value of the `minlen` option in `/etc/security/pwquality.conf` with the following command:

```
# grep minlen /etc/security/pwquality.conf  
minlen = 15
```

If the value of `difok` is set to less than 8 and/or `minclass` is set to less than 4, and/or the value of `maxrepeat` is set to more than 3, and/or the value of `maxclassrepeat` is set to more

than 4, and/or it does not return a `minlen` value of 15 or greater, please refer to the remediation procedure below.

Remediation:

Configure the operating system to require the change of at least 8 of the total number of characters when passwords are changed by setting the `difok` option and the `minclass` option and the `maxrepeat` option and the `maxclassrepeat` and the `minlen` option as defined below.

Add the following lines to `/etc/security/pwquality.conf` (or modify the line to have the required value):

Example: `vim /etc/security/pwquality.conf`

```
difok = 8
minclass = 4
maxrepeat = 3
maxclassrepeat = 4
minlen = 15
```

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204411
Rule ID: SV-204411r603261_rule
STIG ID: RHEL-07-010160
Severity: CAT II

Vul ID: V-204412
Rule ID: SV-204412r603261_rule
STIG ID: RHEL-07-010170
Severity: CAT II

Vul ID: V-204413
Rule ID: SV-204413r603261_rule
STIG ID: RHEL-07-010180
Severity: CAT II

Vul ID: V-204414
Rule ID: SV-204414r603261_rule
STIG ID: RHEL-07-010190
Severity: CAT II

Vul ID: V-204423
Rule ID: SV-204423r603261_rule
STIG ID: RHEL-07-010280
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> 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	4.4 <u>Use Unique Passwords</u> 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.			

5.4.8 Ensure date and time of last successful logon (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.

Check that `pam_lastlog` is used and not silent 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, refer to the remediation procedure below.

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`.

Example: `vim /etc/pam.d/postlogin`

Add the following line to the top of the file:

```
session required pam_lastlog.so showfailed
```

References:

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204605
Rule ID: SV-204605r603261_rule
STIG ID: RHEL-07-040530
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

5.4.9 Ensure multifactor authentication for access to privileged accounts (Automated)

Profile Applicability:

- STIG

Description:

The operating system must implement multifactor authentication for access to privileged accounts via pluggable authentication modules (PAM).

Rationale:

Using an authentication device, such as a 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 Common Access Card.

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 implements multifactor authentication for remote access to privileged accounts via pluggable authentication modules (PAM).

Check the `/etc/sss/sss.conf` file for the authentication services that are being used with the following command:

```
# grep services /etc/sss/sss.conf /etc/sss/conf.d/*.conf  
services = nss, pam
```

If the `pam` service is not present on all `services` lines, refer to the remediation procedure below.

Remediation:

Configure the operating system to implement multifactor authentication for remote access to privileged accounts via PAM.

Modify all of the services lines in `/etc/sss/sss.conf` or in configuration files found under `/etc/sss/conf.d` to include `pam`.

Example: `vim /etc/sss/sss.conf`

Add `pam` to the service line as shown here:

```
services = nss, pam
```

References:

1. CCI-001948: The information system implements multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access
2. NIST SP 800-53 Revision 4 :: IA-2 (11)
3. CCI-001953: The information system accepts Personal Identity Verification (PIV) credentials
4. NIST SP 800-53 Revision 4 :: IA-2 (12)
5. CCI-001954: The information system electronically verifies Personal Identity Verification (PIV) credentials
6. NIST SP 800-53 Revision 4 :: IA-2 (12)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204632
Rule ID: SV-204632r603261_rule
STIG ID: RHEL-07-041002
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>6.5 Require MFA for Administrative Access</u> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.			
v7	<u>16.3 Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

5.4.10 Ensure certificate status checking for PKI authentication (Automated)

Profile Applicability:

- STIG

Description:

The operating system must implement certificate status checking for PKI authentication.

Rationale:

Using an authentication device, such as a 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 Common Access Card.

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 implements certificate status checking for PKI authentication.

Check to see if Online Certificate Status Protocol (OCSP) is enabled on the system with the following command:

```
# grep cert_policy /etc/pam_pkcs11/pam_pkcs11.conf | grep -v "^#"
cert_policy = ca, ocsp_on, signature;
cert_policy = ca, ocsp_on, signature;
cert_policy = ca, ocsp_on, signature;
```

There should be at least 3 lines returned.

If `ocsp_on` is not present in all uncommented `cert_policy` lines in `/etc/pam_pkcs11/pam_pkcs11.conf`, refer to the remediation procedure below.

Remediation:

Configure the operating system to do certificate status checking for PKI authentication. Modify all of the `cert_policy` lines in `/etc/pam_pkcs11/pam_pkcs11.conf` to include `ocsp_on`.

Note: Make sure there is a minimum of 3 `cert_policy` lines.

Example: `vim /etc/pam_pkcs11/pam_pkcs11.conf`

Add, uncomment or update the `cert_policy` lines to include `ocsp_on`:

```
cert_policy = ca, ocsp_on, signature;
cert_policy = ca, ocsp_on, signature;
cert_policy = ca, ocsp_on, signature;
```

References:

1. CCI-001948: The information system implements multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access
2. NIST SP 800-53 Revision 4 :: IA-2 (11)
3. CCI-001953: The information system accepts Personal Identity Verification (PIV) credentials
4. NIST SP 800-53 Revision 4 :: IA-2 (12)
5. CCI-001954: The information system electronically verifies Personal Identity Verification (PIV) credentials
6. NIST SP 800-53 Revision 4 :: IA-2 (12)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204633
Rule ID: SV-204633r603261_rule
STIG ID: RHEL-07-041003
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>6.5 Require MFA for Administrative Access</u> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.			
v7	<u>16.3 Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

5.4.11 Ensure password prohibited reuse is at a minimum 5 (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that passwords are prohibited from reuse for a minimum of 5 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 consecutively reuse their password when that password has exceeded its defined lifetime, the end result is a password that is not changed per policy requirements.

Audit:

Verify the operating system prohibits password reuse for a minimum of 5 generations. Check for the value of the `remember` argument in `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth` with the following command:

```
# grep -i remember /etc/pam.d/system-auth /etc/pam.d/password-auth  
password requisite pam_pwhistory.so use_authtok remember=5 retry=3
```

If the line containing the `pam_pwhistory.so` line 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, refer to the remediation procedure below.

Remediation:

To configure the operating system to prohibit password reuse for a minimum of 5 generations.

Add the following line in `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth` (or modify the line to have the required value):

Example: `vim /etc/pam.d/system-auth`

Add, uncomment or update the following line:

```
password requisite pam_pwhistory.so use_authtok remember=5 retry=3
```

Note: Manual changes to the listed files may be overwritten by the `authconfig` program.

The `authconfig` program should not be used to update the configurations listed in this requirement.

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204422
Rule ID: SV-204422r603261_rule
STIG ID: RHEL-07-010270
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> 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	4.4 <u>Use Unique Passwords</u> 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.			

5.4.12 Ensure accounts lock for a minimum of 15 minutes after three unsuccessful logon attempts within a 15-minute timeframe (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured to lock accounts for a minimum of 15 minutes after three unsuccessful logon attempts within a 15-minute timeframe.

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005

Audit:

Check that the system locks an account for a minimum of 15 minutes after three unsuccessful logon attempts within a period of 15 minutes with the following command:

```
# grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth silent audit deny=3 even_deny_root
fail_interval=900 unlock_time=900
auth [default=die] pam_faillock.so authfail audit deny=3 even_deny_root
fail_interval=900 unlock_time=900
account required pam_faillock.so
```

If the "deny" parameter is set to "0" or a value greater than "3" on both "auth" lines with the "pam_faillock.so" module, or is missing from these lines, this is a finding.

If the "even_deny_root" parameter is not set on both "auth" lines with the "pam_faillock.so" module, or is missing from these lines, this is a finding.

If the "fail_interval" parameter is set to "0" or is set to a value less than "900" on both "auth" lines with the "pam_faillock.so" module, or is missing from these lines, this is a finding.

If the "unlock_time" parameter is not set to "0", "never", or is set to a value less than "900" on both "auth" lines with the "pam_faillock.so" module, or is missing from these lines, this is a finding.

Note: The maximum configurable value for "unlock_time" is "604800".

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 silent audit deny=3 even_deney_root
fail_interval=900 unlock_time=900
auth [default=die] pam_faillock.so authfail audit deny=3 even_deney_root
fail_interval=900 unlock_time=900
account required pam_faillock.so
```

If the "deny" parameter is set to "0" or a value greater than "3" on both "auth" lines with the "pam_faillock.so" module, or is missing from these lines, this is a finding.

If the "even_deney_root" parameter is not set on both "auth" lines with the "pam_faillock.so" module, or is missing from these lines, this is a finding.

If the "fail_interval" parameter is set to "0" or is set to a value less than "900" on both "auth" lines with the "pam_faillock.so" module, or is missing from these lines, this is a finding.

If the "unlock_time" parameter is not set to "0", "never", or is set to a value less than "900" on both "auth" lines with the "pam_faillock.so" module or is missing from these lines, this is a finding.

Note: The maximum configurable value for "unlock_time" is "604800".

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 for the maximum period when three unsuccessful logon attempts in 15 minutes are made.

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 silent audit deny=3 even_deney_root
fail_interval=900 unlock_time=900
auth sufficient pam_unix.so try_first_pass
auth [default=die] pam_faillock.so authfail audit deny=3 even_deney_root
fail_interval=900 unlock_time=900
account required pam_faillock.so
```

Note: Manual changes to the listed files may be overwritten by the "authconfig" program. The "authconfig" program should not be used to update the configurations listed in this requirement.

References:

1. CCI: CCI-000044: The information system enforces the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.
2. NIST SP 800-53 :: AC-7 a
3. NIST SP 800-53A :: AC-7.1 (ii)
4. NIST SP 800-53 Revision 4 :: AC-7 a
5. CCI-002236: The organization defines the time period the information system will automatically lock the account or node when the maximum number of unsuccessful attempts is exceeded.
6. NIST SP 800-53 Revision 4 :: AC-7 b
7. CCI-002237: The organization defines the delay algorithm to be employed by the information system to delay the next login prompt when the maximum number of unsuccessful attempts is exceeded.
8. NIST SP 800-53 Revision 4 :: AC-7 b
9. CCI-002238: The information system automatically locks the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next login prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.
10. NIST SP 800-53 Revision 4 :: AC-7 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204427
Rule ID: SV-204427r603824_rule
STIG ID: RHEL-07-010320
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 <u>Establish an Access Revoking Process</u> 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	16.7 <u>Establish Process for Revoking Access</u> 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.			

5.4.13 Ensure lockout for unsuccessful root logon attempts (Automated)

Profile Applicability:

- STIG

Description:

The operating system must lock the associated account after three unsuccessful root logon attempts are made within a 15-minute period.

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005

Audit:

Verify the operating system automatically locks the `root` account until it is released by an administrator when 3 unsuccessful logon attempts in 15 minutes are made.

```
# grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth silent audit deny=3 even_deney_root
fail_interval=900 unlock_time=900
auth [default=die] pam_faillock.so authfail audit deny=3 even_deney_root
fail_interval=900 unlock_time=900
account required pam_faillock.so
```

If the `even_deney_root` setting is not defined on both lines with the `pam_faillock.so` module, is commented out, or is missing from a line, refer to the remediation procedure below.

```
# grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth silent audit deny=3 even_deney_root
fail_interval=900 unlock_time=900
auth [default=die] pam_faillock.so authfail audit deny=3 even_deney_root
fail_interval=900 unlock_time=900
account required pam_faillock.so
```

If the `even_deney_root` setting is not defined on both lines with the `pam_faillock.so` module, is commented out, or is missing from a line, refer to the remediation procedure below.

Remediation:

To configure the operating system to lock automatically the `root` account until the locked account is released by an administrator when 3 unsuccessful logon attempts in 15 minutes are made.

Modify the first 3 lines of the `auth` section and the first line of the `account` section of the `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth` files to match the following lines:

Example: `vim /etc/pam.d/system-auth`

Add, uncomment or update the following lines in each file:

```
auth required pam_faillock.so preauth silent audit deny=3 even_deny_root
fail_interval=900 unlock_time=900
auth sufficient pam_unix.so try_first_pass
auth [default=die] pam_faillock.so authfail audit deny=3 even_deny_root
fail_interval=900 unlock_time=900
account required pam_faillock.so
```

References:

1. CCI: CCI-002238: The information system automatically locks the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next login prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.
2. NIST SP 800-53 Revision 4 :: AC-7 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204428
Rule ID: SV-204428r603261_rule
STIG ID: RHEL-07-010330
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>6.2 Establish an Access Revoking Process</u> 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	<u>16.7 Establish Process for Revoking Access</u> 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.			

5.5 User Accounts and Environment

This section provides guidance on setting up secure defaults for system and user accounts and their environment.

5.5.1 Set 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.

5.5.1.1 Ensure password expiration is 365 days or less (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. It is recommended that the `PASS_MAX_DAYS` parameter be set to less than or equal to 365 days.

Notes:

- *A value of -1 will disable password expiration.*
- *The password expiration must be greater than the minimum days between password changes or users will be unable to change their password.*

Rationale:

The window of opportunity for an attacker to leverage compromised credentials via a brute force attack, using already compromised credentials, or gaining the credentials by other means, can be limited by the age of the password. Therefore, reducing the maximum age of a password can also reduce an attacker's window of opportunity.

Requiring passwords to be changed helps to mitigate the risk posed by the poor security practice of passwords being used for multiple accounts, and poorly implemented offboarding and change of responsibility policies. This should **not** be considered a replacement for proper implementation of these policies and practices.

Note: If it is believed that a user's password may have been compromised, the user's account should be locked immediately. Local policy should be followed to ensure the secure update of their password.

Audit:

Run the following command and verify `PASS_MAX_DAYS` conforms to site policy (no more than 365 days):

```
# grep ^\s*PASS_MAX_DAYS /etc/login.defs  
PASS_MAX_DAYS 365
```

Run the following command and Review list of users and `PASS_MAX_DAYS` to verify that all users' `PASS_MAX_DAYS` conforms to site policy (no more than 365 days):

```
# grep -E '^[^:]+:[^!]*' /etc/shadow | cut -d: -f1,5  
<user>:<PASS_MAX_DAYS>
```

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>
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process 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	4.4 Use Unique Passwords 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.			

5.5.1.2 Ensure minimum days between password changes is configured (Automated)

Profile Applicability:

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

Description:

The `PASS_MIN_DAYS` parameter in `/etc/login.defs` allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that `PASS_MIN_DAYS` parameter be set to 1 or more days.

Rationale:

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.

Audit:

Run the following command and verify `PASS_MIN_DAYS` conforms to site policy (no less than 1 day):

```
# grep ^\s*PASS_MIN_DAYS /etc/login.defs
PASS_MIN_DAYS 1
```

Run the following command and Review list of users and `PAS_MIN_DAYS` to Verify that all users' `PAS_MIN_DAYS` conforms to site policy (no less than 1 day):

```
# grep -E ^[^:]+:[^!*] /etc/shadow | cut -d: -f1,4
<user>:<PASS_MIN_DAYS>
```

Remediation:

Set the `PASS_MIN_DAYS` parameter to 1 in `/etc/login.defs`:

```
PASS_MIN_DAYS 1
```

Modify user parameters for all users with a password set to match:

```
# chage --mindays 1 <user>
```

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204418
Rule ID: SV-204418r603261_rule
STIG ID: RHEL-07-010230
Severity: CAT II

Vul ID: V-204419
Rule ID: SV-204419r603261_rule
STIG ID: RHEL-07-010240
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process 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	4.4 Use Unique Passwords 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.			

5.5.1.3 Ensure password expiration warning days is 7 or more (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. It is recommended that the `PASS_WARN_AGE` parameter be set to 7 or more days.

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` conforms to site policy (No less than 7 days):

```
# grep ^\s*PASS_WARN_AGE /etc/login.defs
PASS_WARN_AGE 7
```

Verify all users with a password have their number of days of warning before password expires set to 7 or more:

Run the following command and Review list of users and `PASS_WARN_AGE` to verify that all users' `PASS_WARN_AGE` conforms to site policy (No less than 7 days):

```
# grep -E ^[^:]+:[^!*] /etc/shadow | cut -d: -f1,6
<user>:<PASS_WARN_AGE>
```


Remediation:

Set the `PASS_WARN_AGE` parameter to 7 in `/etc/login.defs` :

```
PASS_WARN_AGE 7
```

Modify user parameters for all users with a password set to match:

```
# chage --warndays 7 <user>
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	4.4 <u>Use Unique Passwords</u> 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.			

5.5.1.4 Ensure inactive password lock is 30 days or less (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. It is recommended that accounts that are inactive for 30 days after password expiration be disabled.

Note: A value of -1 would disable this setting.

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 30 days):

```
# useradd -D | grep INACTIVE  
  
INACTIVE=30
```

Verify all users with a password have Password inactive no more than 30 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 30 days):

```
# grep -E ^[^:]+:[^!*] /etc/shadow | cut -d: -f1,7  
  
<user>:<INACTIVE>
```

Remediation:

Run the following command to set the default password inactivity period to 30 days:

```
# useradd -D -f 30
```

Modify user parameters for all users with a password set to match:

```
# chage --inactive 30 <user>
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	16.9 <u>Disable Dormant Accounts</u> Automatically disable dormant accounts after a set period of inactivity.			

5.5.1.5 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 users recorded password change date is in the future then they could bypass any set password expiration.

Audit:

Run the following command and verify nothing is returned

```
# for usr in $(cut -d: -f1 /etc/shadow); do [[ $(chage --list $usr | grep '^Last password change' | cut -d: -f2) > $(date) ]] && echo "$usr :$(chage --list $usr | grep '^Last password change' | cut -d: -f2)"; done
```

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	5.2 Use Unique Passwords 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	4.4 Use Unique Passwords 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.			

5.5.1.6 Ensure shadow file is configured to use only encrypted representations of passwords (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured to use the shadow file to store only encrypted representations of passwords.

Rationale:

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. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Audit:

Verify the system's shadow file is configured to store only encrypted representations of passwords. The strength of encryption that must be used to hash passwords for all accounts is SHA512.

Check that the system is configured to create SHA512 hashed passwords with the following command:

```
# grep -i encrypt /etc/login.defs  
ENCRYPT_METHOD SHA512
```

If the "/etc/login.defs" configuration file does not exist or allows for password hashes other than SHA512 to be used, this is a finding.

Remediation:

Configure the operating system to store only SHA512 encrypted representations of passwords.

Add or update the following line in /etc/login.defs:

```
ENCRYPT_METHOD SHA512
```

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204416
Rule ID: SV-204416r603261_rule
STIG ID: RHEL-07-010210
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> 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	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.			

5.5.1.7 Ensure password expiration is 60 Day maximum for new users (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that passwords for new users 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 passwords could be compromised.

Audit:

If passwords are not being used for authentication, this is Not Applicable.

Verify the operating system enforces a 60-day maximum password lifetime restriction for new user accounts.

Check for the value of `PASS_MAX_DAYS` in `/etc/login.defs` with the following command:

```
# grep -i pass_max_days /etc/login.defs
PASS_MAX_DAYS 60
```

If the `PASS_MAX_DAYS` parameter value is not 60 or less, or is commented out, refer to the remediation procedure below.

Remediation:

Configure the operating system to enforce a 60-day maximum password lifetime restriction.

Add the following line in `/etc/login.defs` (or modify the line to have the required value):

```
PASS_MAX_DAYS 60
```

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204420
Rule ID: SV-204420r603261_rule
STIG ID: RHEL-07-010250
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords 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	4.4 Use Unique Passwords 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.			

5.5.1.8 Ensure password expiration is 60 Day maximum for existing passwords (Automated)

Profile Applicability:

- STIG

Description:

The operating system 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 passwords could be compromised.

Audit:

Check whether the maximum time period for existing passwords is restricted to 60 days.

```
# awk -F: '$5 > 60 {print $1 " " $5}' /etc/shadow
```

If any results are returned that are not associated with a system account, refer to the remediation procedure below.

Remediation:

Configure non-compliant accounts to enforce a 60-day maximum password lifetime restriction.

Using the list of accounts collected in the Audit and run this command on the Users:

```
# chage -M 60 [user]
```

Additional Information:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204421
Rule ID: SV-204421r603261_rule
STIG ID: RHEL-07-010260
Severity: CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> 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	4.4 <u>Use Unique Passwords</u> 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.			

5.5.1.9 Ensure inactive password lock is 0 days (Automated)

Profile Applicability:

- STIG

Description:

The operating system must disable account identifiers (individuals, groups, roles, and devices) if the password expires.

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.

Operating systems need to track periods of inactivity and disable application identifiers after zero days of inactivity.

Audit:

If passwords are not being used for authentication, this is Not Applicable.

Verify the operating system disables account identifiers (individuals, groups, roles, and devices) after the password expires with the following command:

```
# grep -i inactive /etc/default/useradd  
INACTIVE=0
```

If the value is not set to 0, is commented out, or is not defined, refer to the remediation procedure below.

Remediation:

Configure the operating system to disable account identifiers (individuals, groups, roles, and devices) after the password expires.

Add the following line to `/etc/default/useradd` (or modify the line to have the required value):

Example: `vim /etc/default/useradd`

Add, uncomment or update the following line:

```
INACTIVE=0
```

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204426
Rule ID: SV-204426r603261_rule
STIG ID: RHEL-07-010310
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords 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	4.4 Use Unique Passwords 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.			

5.5.1.10 Ensure delay between logon prompts on failure (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that the delay between logon prompts following a failed console logon attempt is at least four seconds.

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 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.

Check the value of the `fail_delay` parameter in the `/etc/login.defs` file 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, refer to the remediation procedure below.

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:

Example: `vim /etc/login.defs`

Add, uncomment or update the following line:

```
FAIL_DELAY 4
```

References:

1. CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204431
Rule ID: SV-204431r603261_rule
STIG ID: RHEL-07-010430
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

5.5.2 Ensure system accounts are secured (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.

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.

Note: The `root`, `sync`, `shutdown`, and `halt` users are exempted from requiring a non-login shell.

Audit:

Run the following commands and verify no results are returned:

```
awk -F: '($1!="root" && $1!="sync" && $1!="shutdown" && $1!="halt" && $1!~/^\/ && $3<"$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)"' && $7!="$(which nologin)"' && $7!="bin/false") {print}' /etc/passwd
awk -F: '($1!="root" && $1!~/^\/ && $3<"$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)"') {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' |
awk '($2!="L" && $2!="LK") {print $1}'
```

Remediation:

Run the commands appropriate for your distribution:

Set the shell for any accounts returned by the audit to nologin:

```
# usermod -s $(which nologin) <user>
```

Lock any non root accounts returned by the audit:

```
# usermod -L <user>
```

The following command will set all system accounts to a non login shell:

```
awk -F: '($1!="root" && $1!="sync" && $1!="shutdown" && $1!="halt" && $1!~/^\/ && $3<"$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)"' && $7!="$(which nologin)"' && $7!="/bin/false" && $7!="/usr/bin/false") {print $1}' /etc/passwd | while read -r user; do usermod -s "$(which nologin)" "$user"; done
```

The following command will automatically lock not root system accounts:

```
awk -F: '($1!="root" && $1!~/^\/ && $3<"$(awk '/^\s*UID_MIN/{print $2}' /etc/login.defs)"') {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' | awk '($2!="L" && $2!="LK") {print $1}' | while read -r user; do usermod -L "$user"; done
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	16 <u>Account Monitoring and Control</u> Account Monitoring and Control			

5.5.3 Ensure default group for the root account is GID 0 (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `usermod` command can be used to specify which group the root user belongs to. This affects permissions of files that are created by the root user.

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 and verify the result is 0 :

```
# grep "^root:" /etc/passwd | cut -f4 -d:
0
```

Remediation:

Run the following command to set the `root` user default group to GID 0 :

```
# usermod -g 0 root
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

5.5.4 Ensure default user shell timeout is configured (Automated)

Profile Applicability:

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

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.

```
#!/bin/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
```

References:

1. CCI-001133: The information system terminates the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity
2. NIST SP 800-53 :: SC-10
3. NIST SP 800-53A :: SC-10.1 (ii)
4. NIST SP 800-53 Revision 4 :: SC-10
5. CCI-002361: The information system automatically terminates a user session after organization-defined conditions or trigger events requiring session disconnect
6. NIST SP 800-53 Revision 4 :: AC-12

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 are also checked. Other methods of setting a timeout exist for other shells not covered here.
- Ensure that the timeout conforms to your local policy.

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204579
Rule ID: SV-204579r646844_rule
STIG ID: RHEL-07-040160
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> 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	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

5.5.5 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` (`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-----`.

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**

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:

- A default 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
- No less restrictive System Wide `umask` is set

Run the following script to verify that a default user `umask` is set enforcing a newly created directories's permissions to be 750 (`drwxr-x---`), and a newly created file's permissions be 640 (`rw-r-----`), or more restrictive:

```
#!/bin/bash

passing=""
grep -Eiq '^\s*UMASK\s+(0[0-7][2-7]7|[0-7][2-7]7)\b' /etc/login.defs && grep
-Eqi '^\s*USERGROUPS_ENAB\s*"?no"?\b' /etc/login.defs && grep -Eq
'^\s*session\s+(optional|required)\s+pam_umask\.so\b'
/etc/pam.d/common-session && passing=true
grep -REiq '^\s*UMASK\s+\s*(0[0-7][2-7]7|[0-7][2-
7]7|u=(r?|w?|x?) (r?|w?|x?) (r?|w?|x?),g=(r?x?|x?r?),o=)\b' /etc/profile*
/etc/bashrc* && passing=true
[ "$passing" = true ] && echo "Default user umask is set"
```

Verify output is: "Default user umask is set"

Run the following to verify that no less restrictive system wide `umask` is set:

```
# grep -Rpi ' (^|^#)*\s*umask\s+([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=[rx]{0,3},)?(g=[rx]{0,3},)?o=[rx]+\b|(u=[rx]{1,3},)?g=[^rx]{1,3}(
,o=[rx]{0,3})?\b)' /etc/login.defs /etc/profile* /etc/bashrc*

No file should be returned
```


Remediation:

Review `/etc/bashrc`, `/etc/profile`, and all files ending in `*.sh` in the `/etc/profile.d/` directory and remove or edit all `umask` entries to follow local site policy. Any remaining entries should be: `umask 027`, `umask u=rwx,g=rx,o=` or more restrictive.

Configure `umask` in **one** of the following files:

- A file in the `/etc/profile.d/` directory ending in `.sh`
- `/etc/profile`
- `/etc/bashrc`

Example:

```
# vi /etc/profile.d/set_umask.sh

umask 027
```

Run the following command and remove or modify the `umask` of any returned files:

```
# grep -RPi ' (^|^ [^#]*) \s*umask\s+ ([0-7] [0-7] [01] [0-7] \b| [0-7] [0-7] [0-7] [0-7] \b| [0-7] [01] [0-7] \b| [0-7] [0-7] [0-6] \b| [0-7] [01] [0-7] \b| [0-7] [0-7] [0-6] \b| (u=[rwx]{0,3},)? (g=[rwx]{0,3},)? o=[rwx]+\b| (u=[rwx]{1,3},)? g=[^rx]{1,3} (,o=[rwx]{0,3})?\b)' /etc/login.defs /etc/profile* /etc/bashrc*
```

Follow one of the following methods to set the default user `umask`:

Edit `/etc/login.defs` and edit the `UMASK` and `USERGROUPS_ENAB` lines as follows:

```
UMASK 027

USERGROUPS_ENAB no
```

Edit the files `/etc/pam.d/password-auth` and `/etc/pam.d/system-auth` and add or edit the following:

```
session      optional      pam_umask.so
```

OR Configure `umask` in one of the following files:

- A file in the `/etc/profile.d/` directory ending in `.sh`
- `/etc/profile`
- `/etc/bashrc`

Example: `/etc/profile.d/set_umask.sh`

```
umask 027
```

Note: 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.

Default Value:

UMASK 022

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	3.3 <u>Configure Data Access Control Lists</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			
v7	13 <u>Data Protection</u> Data Protection			

5.5.6 Ensure user and group account administration utilities are configured to store only encrypted representations of passwords (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that user and group account administration utilities are configured to store only encrypted representations of passwords.

Rationale:

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. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Audit:

Verify the user and group account administration utilities are configured to store only encrypted representations of passwords. The strength of encryption that must be used to hash passwords for all accounts is "SHA512".

Check that the system is configured to create "SHA512" hashed passwords with the following command:

```
# grep -i sha512 /etc/libuser.conf  
crypt_style = sha512
```

If the "crypt_style" variable is not set to "sha512", is not in the defaults section, is commented out, or does not exist, this is a finding.

Remediation:

Configure the operating system to store only SHA512 encrypted representations of passwords.

Add or update the following line in "/etc/libuser.conf" in the [defaults] section:

```
crypt_style = sha512
```

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204417
Rule ID: SV-204417r603261_rule
STIG ID: RHEL-07-010220
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> 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	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.			

5.5.7 Ensure multi-factor authentication is enable for users (Automated)

Profile Applicability:

- STIG

Description:

The operating system must uniquely identify and must authenticate organizational users (or processes acting on behalf of organizational users) using multi-factor authentication.

Rationale:

To assure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1. Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication;
- and
2. Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Audit:

Verify the operating system requires organizational users to use multifactor authentication.
Check to see if smartcard authentication is enforced on the system:

```
# authconfig --test | grep "pam_pkcs11 is enabled"
```

If no results are returned, refer to the remediation procedure below.
Check to see if smartcard removal action is set:

```
# authconfig --test | grep "smartcard removal action"
```

If smartcard removal action is blank, refer to the remediation procedure below.
Check to see if smartcard module is set:

```
# authconfig --test | grep "smartcard module"
```

If smartcard module is blank, refer to the remediation procedure below.

Remediation:

Configure the operating system to require individuals to be authenticated with a multifactor authenticator.

Enable smartcard logons with the following commands:

```
# authconfig --enablesmartcard --smartcardaction=0 --update  
# authconfig --enablerequiresmartcard --update
```

Modify the `/etc/pam_pkcs11/pkcs11_eventmgr.conf` file to uncomment the following line:

Example: `vim /etc/pam_pkcs11/pkcs11_eventmgr.conf`

Uncomment the following line:

```
/usr/X11R6/bin/xscreensaver-command -lock
```

Note: Modify the `/etc/pam_pkcs11/pam_pkcs11.conf` file to use the cackey module if required.

References:

1. CCI: CCI-000766: The information system implements multifactor authentication for network access to non-privileged accounts.
2. NIST SP 800-53 :: IA-2 (2)
3. NIST SP 800-53A :: IA-2 (2).1
4. NIST SP 800-53 Revision 4 :: IA-2 (2)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204441
Rule ID: SV-204441r603261_rule
STIG ID: RHEL-07-010500
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.5 <u>Require MFA for Administrative Access</u> 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> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

5.5.8 Ensure Default user umask is 077 (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:

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, refer to the remediation procedure below.

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`:

Example: `vim /etc/login.defs`

Add, uncomment or update the following line:

```
UMASK 077
```


References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204457
Rule ID: SV-204457r603261_rule
STIG ID: RHEL-07-020240
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

5.5.9 Ensure local interactive user accounts umask is 077 (Automated)

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 700 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 -i umask /home/*/*.*
```

If any local interactive user initialization (`dot`) files are found to have a umask statement that has a value less restrictive than 077, refer to the remediation procedure below.

Remediation:

Remove the umask statement from all local interactive user's initialization files.

Using the list collected in the audit run the following command on all the files located with a less restrictive umask:

```
user@server# ~]$ echo 'umask 077' [] /home/user/path_to_file
```

If the account is for an application, the requirement for a umask less restrictive than 077 can be documented, 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. CCI-000318: The organization audits and reviews activities associated with configuration controlled changes to the system.
2. NIST SP 800-53 :: CM-3 e
3. NIST SP 800-53A :: CM-3.1 (v)
4. NIST SP 800-53 Revision 4 :: CM-3 f
5. CCI-000368: The organization documents any deviations from the established configuration settings for organization-defined information system components based on organization-defined operational requirements.
6. NIST SP 800-53 :: CM-6 c
7. NIST SP 800-53A :: CM-6.1 (v)
8. NIST SP 800-53 Revision 4 :: CM-6 c
9. CCI-001812: The information system prohibits user installation of software without explicit privileged status.
10. NIST SP 800-53 Revision 4 :: CM-11 (2)
11. CCI-001813: The information system enforces access restrictions.
12. NIST SP 800-53 Revision 4 :: CM-5 (1)
13. CCI-001814: The Information system supports auditing of the enforcement actions.
14. NIST SP 800-53 Revision 4 :: CM-5 (1)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204488
Rule ID: SV-204488r603261_rule
STIG ID: RHEL-07-021040
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

5.5.10 Ensure upon user creation a home directory is assigned. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that all local interactive user accounts, upon creation, are assigned a home directory.

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 on the system are assigned a home directory upon creation.

Check to see if the system is configured to create home directories for local interactive users 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, refer to the remediation procedure below.

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.

Example: `vim /etc/login.defs`

Add, uncomment or update the following line:

```
CREATE_HOME yes
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204466
Rule ID: SV-204466r603261_rule
STIG ID: RHEL-07-020610
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

5.6 Ensure root login is restricted to system console (Manual)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The file `/etc/securetty` contains a list of valid terminals that may be logged in directly as root.

Rationale:

Since the system console has special properties to handle emergency situations, it is important to ensure that the console is in a physically secure location and that unauthorized consoles have not been defined.

Audit:

```
# cat /etc/securetty
```

Remediation:

Remove entries for any consoles that are not in a physically secure location.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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.			
v8	<u>4.6 Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v7	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

5.7 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
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

6 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.

6.1 System File Permissions

This section provides guidance on securing aspects of system files and directories.

6.1.1 Audit system file permissions (Manual)

Profile Applicability:

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

Description:

The RPM package manager has a number of useful options. One of these, the `-v` option, can be used to verify that system packages are correctly installed. The `v` option can be used to verify a particular package or to verify all system packages. If no output is returned, the package is installed correctly. The following table describes the meaning of output from the verify option:

Code	Meaning
S	File size differs.
M	File mode differs (includes permissions and file type).
5	The MD5 checksum differs.
D	The major and minor version numbers differ on a device file.
L	A mismatch occurs in a link.
U	The file ownership differs.
G	The file group owner differs.
T	The file time (mtime) differs.

The `rpm -qf` command can be used to determine which package a particular file belongs to. For example the following commands determines which package the `/etc/ssh/sshd_config` file belongs to:

```
# rpm -qf /etc/ssh/sshd_config
openssh-server-7.4p1-21.el7.x86_64
```

To verify the settings for the package that controls the `/bin/bash` file, run the following:

```
# rpm -V openssh-server-7.4p1-21.el7.x86_64
S.5....T.  c /etc/ssh/sshd_config
```

Note: You can feed the output of the `rpm -qf` command to the `rpm -V` command:

```
# rpm -V $(rpm -qf /etc/ssh/sshd_config)
S.5....T.  c /etc/ssh/sshd_config
```

Notes:

- *Since packages and important files may change with new updates and releases, it is recommended to verify everything, not just a finite list of files. This can be a time consuming task and results may depend on site policy therefore it is not a scorable benchmark item, but is provided for those interested in additional security measures.*
- *Some of the recommendations of this benchmark alter the state of files audited by this recommendation. The audit command will alert for all changes to a file permissions even if the new state is more secure than the default.*

Rationale:

It is important to confirm that packaged system files and directories are maintained with the permissions they were intended to have from the OS distributor or in accordance with local site policy.

Audit:

Run the following command to review all installed packages. Note that this may be very time consuming and may be best scheduled via the `cron` utility. It is recommended that the output of this command be redirected to a file that can be reviewed later. This command will ignore configuration files due to the extreme likelihood that they will change.

```
# rpm -Va --nomtime --nosize --nomd5 --nolinkto > <filename> | grep -vw c
```

Remediation:

Investigate the results to ensure any discrepancies found are understood and support proper secure operation of the system.

References:

1. <https://docs.fedoraproject.org/en-US/fedora/rawhide/system-administrators-guide/RPM/#s2-rpm-verifying>
2. CCI-001749: The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization
3. NIST SP 800-53 Revision 4 :: CM-5 (3)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-214799
Rule ID: SV-214799r603261_rule
STIG ID: RHEL-07-010020
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

6.1.2 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 and verify `Uid` and `Gid` are both `0/root` and `Access` is `644` or more restrictive:

```
# stat /etc/passwd
Access: (0644/-rw-r--r--)  Uid: (    0/   root)   Gid: (    0/   root)
```

Remediation:

Run the following commands to set owner, group, and permissions on `/etc/passwd`:

```
# chown root:root /etc/passwd
# chmod u-x,g-wx,o-wx /etc/passwd
```


CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>14.6 Protect Information through Access Control Lists</u> 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.			

6.1.3 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 and verify Uid and Gid are both 0/root and Access is 644 or more restrictive:

```
# stat /etc/passwd-  
Access: (0644/-rw-----)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set owner, group, and permissions on /etc/passwd- :

```
# chown root:root /etc/passwd-  
# chmod u-x,go-wx /etc/passwd-
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

6.1.4 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 and verify Uid and Gid are 0/root , and Access is 0000 :

```
# stat /etc/shadow
Access: (0000/-----)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set owner, group, and permissions on `/etc/shadow` :

```
# chown root:root /etc/shadow
# chmod 0000 /etc/shadow
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>14.6 Protect Information through Access Control Lists</u> 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.			

6.1.5 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 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 and verify Uid is 0/root, Gid is 0/root and Access is 0000 :

```
# stat /etc/shadow-  
Access: (0000/-----)  Uid: (    0/    root)  Gid: (    0/    root)
```

Remediation:

Run the following commands to set owner, group, and permissions on `/etc/shadow-` :

```
# chown root:root /etc/shadow-  
# chmod 0000 /etc/shadow-
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>14.6 Protect Information through Access Control Lists</u> 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.			

6.1.6 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 and verify `Uid` is `0/root`, `Gid` is `0/root` and `Access` is `0000` :

```
# stat /etc/gshadow-  
Access: (0000/-----)  Uid: (    0/    root)  Gid: (    0/    root)
```

Remediation:

Run the following commands to set owner, group, and permissions on `/etc/gshadow-` :

```
# chown root:root /etc/gshadow-  
# chmod 0000 /etc/gshadow-
```


CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.			

6.1.7 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 and verify `Uid` is `0/root`, `Gid` is `0/root` and `Access` is `0000` :

```
# stat /etc/gshadow
Access: (0000/-----)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set owner, group, and permissions on `/etc/gshadow` :

```
# chown root:root /etc/gshadow
# chmod 0000 /etc/gshadow
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>14.6 Protect Information through Access Control Lists</u> 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.			

6.1.8 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 and verify `Uid` and `Gid` are both `0/root` and `Access` is `644` or more restrictive:

```
# stat /etc/group
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
```

Remediation:

Run the following commands to set owner, group, and permissions on `/etc/group` :

```
# chown root:root /etc/group
# chmod u-x,g-wx,o-wx /etc/group
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>14.6 Protect Information through Access Control Lists</u> 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.			

6.1.9 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 and verify `Uid` and `Gid` are both `0/root` and `Access` is `644` or more restrictive:

```
# stat /etc/group-  
Access: (0644/-rw-r--r--)  Uid: (   0/   root)   Gid: (   0/   root)
```

Remediation:

Run the following commands to set owner, group, and permissions on `/etc/group-`:

```
# chown root:root /etc/group-  
# chmod u-x,go-wx /etc/group-
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

6.1.10 Ensure no world writable files exist (Automated)

Profile Applicability:

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

Description:

Unix-based systems support variable settings to control access to files. World writable files are the least secure. See the `chmod(2)` man page for more information.

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.

Audit:

Run the following command and verify no files are returned:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type f -perm -0002
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -type f -perm -0002
```

Remediation:

Removing write access for the "other" category (`chmod o-w <filename>`) is advisable, but always consult relevant vendor documentation to avoid breaking any application dependencies on a given file.

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204478
Rule ID: SV-204478r603261_rule
STIG ID: RHEL-07-020730
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

6.1.11 Ensure no unowned files or directories exist (Automated)

Profile Applicability:

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

Description:

Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system.

Rationale:

A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Audit:

Run the following command and verify no files are returned:

```
# df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -nouser
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -nouser
```

Remediation:

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

References:

1. CCI: CCI-002165: The information system enforces organization-defined discretionary access control policies over defined subjects and objects.
2. NIST SP 800-53 Revision 4 :: AC-3 (4)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204463
Rule ID: SV-204463r603261_rule
STIG ID: RHEL-07-020320
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>13.2 Remove Sensitive Data or Systems Not Regularly Accessed by Organization</u> Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.			

6.1.12 Ensure no ungrouped files or directories exist (Automated)

Profile Applicability:

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

Description:

Sometimes when administrators delete users or groups from the system they neglect to remove all files owned by those users or groups.

Rationale:

A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Audit:

Run the following command and verify no files are returned:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -nogroup
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -nogroup
```

Remediation:

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

References:

1. CCI: CCI-002165: The information system enforces organization-defined discretionary access control policies over defined subjects and objects.
2. NIST SP 800-53 Revision 4 :: AC-3 (4)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204464
Rule ID: SV-204464r603261_rule
STIG ID: RHEL-07-020330
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>13.2 Remove Sensitive Data or Systems Not Regularly Accessed by Organization</u> Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.			

6.1.13 Audit SUID executables (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 program is to enable users to perform functions (such as changing their password) that require root privileges.

Rationale:

There are valid reasons for SUID programs, but it is important to identify and review such programs to ensure they are legitimate.

Audit:

Run the following command to list SUID files:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type f -perm -4000
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -type f -perm -4000
```

Remediation:

Ensure that no rogue SUID 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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

6.1.14 Audit SGID executables (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 SGID program is to enable users to perform functions (such as changing their password) that require root privileges.

Rationale:

There are valid reasons for 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 md5 checksum than what from the package. This is an indication that the binary may have been replaced.

Audit:

Run the following command to list SGID files:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type f -perm -2000
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -type f -perm -2000
```

Remediation:

Ensure that no rogue 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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

6.1.15 Ensure the file permissions ownership and group membership of system files and commands match the vendor values (Manual)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that the file permissions, ownership, and group membership of system files and commands match the vendor values

Rationale:

Discretionary access control is weakened if a user or group has access permissions to system files and directories greater than the default.

Satisfies: SRG-OS-000257-GPOS-00098, SRG-OS-000278-GPOS-00108

Audit:

Verify the file permissions, ownership, and group membership of system files and commands match the vendor values.

Check the default file permissions, ownership, and group membership of system files and commands with the following command:

```
# for i in `rpm -Va | egrep '^.{1}M|^.{5}U|^.{6}G' | cut -d " " -f 4,5`;do
for j in `rpm -qf $i`;do rpm -ql $j --dump | cut -d " " -f 1,5,6,7 | grep
$i;done;done

/var/log/gdm 040755 root root
/etc/audisp/audisp-remote.conf 0100640 root root
/usr/bin/passwd 0104755 root root
```

For each file returned, verify the current permissions, ownership, and group membership:

```
# ls -la <filename>

-rw-----. 1 root root 133 Jan 11 13:25 /etc/audisp/audisp-remote.conf
```

If the file is more permissive than the default permissions, this is a finding.

If the file is not owned by the default owner and is not documented with the Information System Security Officer (ISSO), this is a finding.

If the file is not a member of the default group and is not documented with the Information System Security Officer (ISSO), this is a finding.

Remediation:

Run the following command to determine which package owns the file:

```
# rpm -qf <filename>
```

Reset the user and group ownership of files within a package with the following command:

```
# rpm --setugids <packagename>
```

Reset the permissions of files within a package with the following command:

```
# rpm --setperms <packagename>
```

References:

1. NIST SP 800-53 :: AU-9
2. NIST SP 800-53A :: AU-9.1
3. NIST SP 800-53 Revision 4 :: AU-9
4. NIST SP 800-53 :: AU-9 (3)
5. NIST SP 800-53A :: AU-9 (3).1
6. NIST SP 800-53 Revision 4 :: AU-9 (3)
7. NIST SP 800-53 Revision 4 :: AC-3 (4)
8. NIST SP 800-53 Revision 4 :: AC-6 (10)

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204392
Rule ID: SV-204392r646841_rule
STIG ID: RHEL-07-010010
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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.			

6.1.16 Ensure all world-writable directories are owned by root, sys, bin, or an application User Identifier (Manual)

Profile Applicability:

- STIG

Description:

The Linux operating system must be configured so that all world-writable directories are 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, assuming 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. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-228563
Rule ID: SV-228563r744119_rule
STIG ID: RHEL-07-021031
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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 User and Group Settings

This section provides guidance on securing aspects of the 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.

6.2.1 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.

Notes:

- *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 $1 " is not set to shadowed passwords " }' /etc/passwd
```

Remediation:

If any accounts in the `/etc/passwd` file do not have a single `x` in the password field, run the following command to set these accounts to use shadowed passwords:

```
# sed -e 's/^\([a-zA-Z0-9_]*\) :[^:]*:/\1:x:/' -i /etc/passwd
```

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> 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	4.4 <u>Use Unique Passwords</u> 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.			

6.2.2 Ensure /etc/shadow password fields are not empty (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> 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	4.4 <u>Use Unique Passwords</u> 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.			

6.2.3 Ensure all groups in /etc/passwd exist in /etc/group (Automated)

Profile Applicability:

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

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 and verify no results are returned:

```
#!/bin/bash

for i in $(cut -s -d: -f4 /etc/passwd | sort -u ); do
    grep -q -P "^.*?:[^:]*:$i:" /etc/group
    if [ $? -ne 0 ]; then
        echo "Group $i is referenced by /etc/passwd but does not exist in
/etc/group"
    fi
done
```

Remediation:

Analyze the output of the Audit step above and perform the appropriate action to correct any discrepancies found.

References:

1. CCI: CCI-000764: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).
2. NIST SP 800-53 :: IA-2
3. NIST SP 800-53A :: IA-2.1
4. NIST SP 800-53 Revision 4 :: IA-2

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204461
Rule ID: SV-204461r603261_rule
STIG ID: RHEL-07-020300
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	16 <u>Account Monitoring and Control</u> Account Monitoring and Control			

6.2.4 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 $NF}' /etc/group
# awk -F: -v GID="$(awk -F: '($1=="shadow") {print $3}' /etc/group)"
'($4==GID) {print $1}' /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>
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

6.2.5 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:

```
#!/bin/bash

cut -d: -f1 /etc/passwd | sort | uniq -d | while read x; do
    echo "Duplicate login name ${x} in /etc/passwd"
done
```

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	16 <u>Account Monitoring and Control</u> Account Monitoring and Control			

6.2.6 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:

```
#!/bin/bash

cut -d: -f1 /etc/group | sort | uniq -d | while read -r x; do
    echo "Duplicate group name ${x} in /etc/group"
done
```

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	16 <u>Account Monitoring and Control</u> Account Monitoring and Control			

6.2.7 Ensure no duplicate UIDs exist (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

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.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

cut -f3 -d":" /etc/passwd | sort -n | uniq -c | while read -r x; do
    [ -z "$x" ] && break
    set - "$x"
    if [ "$1" -gt 1 ]; then
        users=$(awk -F: '($3 == n) { print $1 }' n="$2" /etc/passwd | xargs)
        echo "Duplicate UID ($2): $users"
    fi
done
```

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>16 Account Monitoring and Control</u> Account Monitoring and Control			

6.2.8 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.

Note: You can also use the `grpck` command to check for other inconsistencies in the `/etc/group` file.

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:

```
#!/bin/bash
cut -d: -f3 /etc/group | sort | uniq -d | while read -r x; do
    echo "Duplicate GID ($x) in /etc/group"
done
```

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.

Additional Information:

You can also use the `grpck` command to check for other inconsistencies in the `/etc/group` file.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>16 Account Monitoring and Control</u> Account Monitoring and Control			

6.2.9 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:

Remove any users other than `root` with UID 0 or assign them a new UID if appropriate.

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204462
Rule ID: SV-204462r603261_rule
STIG ID: RHEL-07-020310
Severity: CAT I

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

6.2.10 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 and verify no results are returned:

```
#!/bin/bash

RPCV="$(sudo -Hiu root env | grep '^PATH' | cut -d= -f2)"
echo "$RPCV" | grep -q "::-" && echo "root's path contains a empty directory (::)"
echo "$RPCV" | grep -q ":$" && echo "root's path contains a trailing (:)"
for x in $(echo "$RPCV" | tr ":" " "); do
    if [ -d "$x" ]; then
        ls -ldH "$x" | awk '$9 == "." {print "PATH contains current working directory (.)."}'
        $3 != "root" {print $9, "is not owned by root"}
        substr($1,6,1) != "-" {print $9, "is group writable"}
        substr($1,9,1) != "-" {print $9, "is world writable"}
    else
        echo "$x is not a directory"
    fi
done
```

Remediation:

Correct or justify any items discovered in the Audit step.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

6.2.11 Ensure all users' home directories exist (Automated)

Profile Applicability:

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

Description:

Users can be defined in `/etc/passwd` without a home directory or with a home directory that does not actually exist.

Rationale:

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 and verify no results are returned:

```
#!/bin/bash

awk -F: '($1!~/ (halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\usr)?\sbin\nologin(\)?$/ && $7!~/(\usr)?\bin\false(\)?$/ ) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
    if [ ! -d "$dir" ]; then
        echo "User: \"$user\" home directory: \"$dir\" does not exist."
    fi
done
```

Note: The audit script checks all users with interactive shells except `halt`, `sync`, `shutdown`, and `nfsnobody`.

Remediation:

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users without an assigned home directory should be removed or assigned a home directory as appropriate.

The following script will create a home directory for users with an interactive shell whose home directory doesn't exist:

```
#!/bin/bash

awk -F: '($1!~/ (halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\ /usr)?\ /sbin\ /nologin(\ /)?$/ && $7!~/(\ /usr)?\ /bin\ /false(\ /)?$/ ) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
    if [ ! -d "$dir" ]; then
        mkdir "$dir"
        chmod g-w,o-wrx "$dir"
        chown "$user" "$dir"
    fi
done
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204467
Rule ID: SV-204467r603826_rule
STIG ID: RHEL-07-020620
Severity: CAT II

Vul ID: V-204493
Rule ID: SV-204493r603840_rule
STIG ID: RHEL-07-021310
Severity: CAT III

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

6.2.12 Ensure users own their home directories (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.

Rationale:

Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

awk -F: '($1!~/ (halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\ /usr)?\ /sbin\ /nologin(\ )?$/ && $7!~/(\ /usr)?\ /bin\ /false(\ )?$/ ) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
    if [ ! -d "$dir" ]; then
        echo "User: \"$user\" home directory: \"$dir\" does not exist."
    else
        owner=$(stat -L -c "%U" "$dir")
        if [ "$owner" != "$user" ]; then
            echo "User: \"$user\" home directory: \"$dir\" is owned by
\"$owner\""
        fi
    fi
done
```

Remediation:

Change the ownership of any home directories that are not owned by the defined user to the correct user.

The following script will create missing home directories, set the owner, and set the permissions for interactive users' home directories:

```
#!/bin/bash

awk -F: '($1~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\|usr)?\|sbin\|nologin(\|)?$/ && $7!~/^(\|usr)?\|bin\|false(\|)?$/ ) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
    if [ ! -d "$dir" ]; then
        echo "User: \"$user\" home directory: \"$dir\" does not exist, creating
home directory"
        mkdir "$dir"
        chmod g-w,o-rwx "$dir"
        chown "$user" "$dir"
    else
        owner=$(stat -L -c "%U" "$dir")
        if [ "$owner" != "$user" ]; then
            chmod g-w,o-rwx "$dir"
            chown "$user" "$dir"
        fi
    fi
done
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204469
Rule ID: SV-204469r603830_rule
STIG ID: RHEL-07-020640
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

6.2.13 Ensure users' home directories permissions are 750 or more restrictive (Automated)

Profile Applicability:

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

Description:

While the system administrator can establish secure permissions for users' home directories, the users can easily override these.

Rationale:

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.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

awk -F: '($1~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\usr)?\sbin\nologin(\)?$/ && $7!~/(\usr)?\bin\false(\)?$/)
{print $1 " " $6}' /etc/passwd | while read -r user dir; do
    if [ ! -d "$dir" ]; then
        echo "User: \"$user\" home directory: \"$dir\" doesn't exist"
    else
        dirperm=$(stat -L -c "%A" "$dir")
        if [ "$(echo "$dirperm" | cut -c6)" != "-" ] || [ "$(echo "$dirperm" |
cut -c8)" != "-" ] || [ "$(echo "$dirperm" | cut -c9)" != "-" ] || [ "$(echo
"$dirperm" | cut -c10)" != "-" ]; then
            echo "User: \"$user\" home directory: \"$dir\" has permissions:
\"$(stat -L -c "%a" "$dir")\"
        fi
    fi
done
```

Remediation:

Making global modifications to user home directories 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 file permissions and determine the action to be taken in accordance with site policy.

The following script can be used to remove permissions in excess of 750 from users' home directories:

```
#!/bin/bash

awk -F: '($1!~/ (halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\ /usr)?\ /sbin\ /nologin(\ /)?$/ && $7!~/^(\ /usr)?\ /bin\ /false(\ /)?$/ )
{print $6}' /etc/passwd | while read -r dir; do
    if [ -d "$dir" ]; then
        dirperm=$(stat -L -c "%A" "$dir")
        if [ "$(echo "$dirperm" | cut -c6)" != "-" ] || [ "$(echo "$dirperm" |
cut -c8)" != "-" ] || [ "$(echo "$dirperm" | cut -c9)" != "-" ] || [ "$(echo
"$dirperm" | cut -c10)" != "-" ]; then
            chmod g-w,o-rwx "$dir"
        fi
    fi
done
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204468
Rule ID: SV-204468r603828_rule
STIG ID: RHEL-07-020630
Severity: CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>14.6 Protect Information through Access Control Lists</u> 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.			

6.2.14 Ensure users' dot files are not group or world writable (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.

Rationale:

Group or world-writable user configuration files may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

awk -F: '($1!~/ (halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\ /usr)?\ /sbin\ /nologin(\ /)?$/ && $7!~/^(\ /usr)?\ /bin\ /false(\ /)?$/ ) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
    if [ -d "$dir" ]; then
        for file in "$dir"/*; do
            if [ ! -h "$file" ] && [ -f "$file" ]; then
                fileperm=$(stat -L -c "%A" "$file")
                if [ "$(echo "$fileperm" | cut -c6)" != "-" ] || [ "$(echo
"$fileperm" | cut -c9)" != "-" ]; then
                    echo "User: \"$user\" file: \"$file\" has permissions:
\"$fileperm\""
                fi
            fi
        done
    fi
done
```

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.

```
#!/bin/bash

awk -F: '($1!~/ (halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\ /usr)?\ /sbin\ /nologin(\ /)?$/ && $7!~/(\ /usr)?\ /bin\ /false(\ /)?$/ ) {
print $6 }' /etc/passwd | while read -r dir; do
    if [ -d "$dir" ]; then
        for file in "$dir"/*.*; do
            if [ ! -h "$file" ] && [ -f "$file" ]; then
                fileperm=$(stat -L -c "%A" "$file")
                if [ "$(echo "$fileperm" | cut -c6)" != "-" ] || [ "$(echo
"$fileperm" | cut -c9)" != "-" ]; then
                    chmod go-w "$file"
                fi
            fi
        done
    fi
done
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

6.2.15 Ensure no users have .forward files (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `.forward` file specifies an email address to forward the user's mail to.

Rationale:

Use of the `.forward` file poses a security risk in that sensitive data may be inadvertently transferred outside the organization. The `.forward` file also poses a risk as it can be used to execute commands that may perform unintended actions.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

awk -F: '($1~/^(root|halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\usr)?\sbin\nologin(\)?$/ && $7!~/(\usr)?\bin\false(\)?$/ ) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
    if [ -d "$dir" ]; then
        file="$dir/.forward"
        if [ ! -h "$file" ] && [ -f "$file" ]; then
            echo "User: \"$user\" file: \"$file\" exists"
        fi
    fi
done
```

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 `.forward` files and determine the action to be taken in accordance with site policy.

The following script will remove `.forward` files from interactive users' home directories

```
#!/bin/bash

awk -F: '($1!~/ (root|halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\usr)?\sbin\nologin(\/)?$/ && $7!~/(\usr)?\bin\false(\/)?$/ ) {
print $6 }' /etc/passwd | while read -r dir; do
    if [ -d "$dir" ]; then
        file="$dir/.forward"
        [ ! -h "$file" ] && [ -f "$file" ] && rm -f "$file"
    fi
done
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

6.2.16 Ensure no users have .netrc files (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `.netrc` file contains data for logging into a remote host for file transfers via FTP.

While the system administrator can establish secure permissions for users' `.netrc` files, the users can easily override these.

Rationale:

The `.netrc` file presents a significant security risk since it stores passwords in unencrypted form. Even if FTP is disabled, user accounts may have brought over `.netrc` files from other systems which could pose a risk to those systems.

If a `.netrc` file is required, and follows local site policy, it should have permissions of `600` or more restrictive.

Audit:

Run the following script. This script will return:

- **FAILED:** for any .netrc file with permissions less restrictive than 600
- **WARNING:** for any .netrc files that exist in interactive users' home directories.

```
#!/bin/bash

awk -F: '($1!~/ (halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\usr)?\sbin\nologin(\)?$/ && $7!~/(\usr)?\bin\false(\)?$/ ) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
    if [ -d "$dir" ]; then
        file="$dir/.netrc"
        if [ ! -h "$file" ] && [ -f "$file" ]; then
            if stat -L -c "%A" "$file" | cut -c4-10 | grep -Eq '[-]+'; then
                echo "FAILED: User: \"$user\" file: \"$file\" exists with
permissions: \"$(stat -L -c "%a" "$file")\", remove file or excessive
permissions"
            else
                echo "WARNING: User: \"$user\" file: \"$file\" exists with
permissions: \"$(stat -L -c "%a" "$file")\", remove file unless required"
            fi
        fi
    fi
done
```

Verify:

- Any lines beginning with **FAILED:** - File should be removed unless deemed necessary, in accordance with local site policy, and permissions are updated to be 600 or more restrictive
- Any lines beginning with **WARNING:** - File should be removed unless deemed necessary, and in accordance with local site policy

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 `.netrc` files and determine the action to be taken in accordance with site policy.

The following script will remove `.netrc` files from interactive users' home directories

```
#!/bin/bash

awk -F: '($1!~/ (halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\ /usr)?\ /sbin\ /nologin(\ /)?$/ && $7!~/(\ /usr)?\ /bin\ /false(\ /)?$/ ) {
print $6 }' /etc/passwd | while read -r dir; do
    if [ -d "$dir" ]; then
        file="$dir/.netrc"
        [ ! -h "$file" ] && [ -f "$file" ] && rm -f "$file"
    fi
done
```

Additional Information:

While the complete removal of `.netrc` files is recommended, if any are required on the system secure permissions must be applied.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.			

6.2.17 Ensure no users have .rhosts files (Automated)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

While no `.rhosts` files are shipped by default, users can easily create them.

Rationale:

This action is only meaningful if `.rhosts` support is permitted in the file `/etc/pam.conf`. Even though the `.rhosts` files are ineffective if support is disabled in `/etc/pam.conf`, they may have been brought over from other systems and could contain information useful to an attacker for those other systems.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

awk -F: '($1!~/ (root|halt|sync|shutdown|nfsnobody)/ &&
$7!~/^ (\/usr)?\/sbin\/nologin(\/)?$/ && $7!~/ (\/usr)?\/bin\/false(\/)?$/ ) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
    if [ -d "$dir" ]; then
        file="$dir/.rhosts"
        if [ ! -h "$file" ] && [ -f "$file" ]; then
            echo "User: \"$user\" file: \"$file\" exists"
        fi
    fi
done
```

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 `.rhosts` files and determine the action to be taken in accordance with site policy.

The following script will remove `.rhosts` files from interactive users' home directories

```
#!/bin/bash

awk -F: '($1!~/ (root|halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\usr)?\sbin\nologin(\/)?$/ && $7!~/(\usr)?\bin\false(\/)?$/ ) {
print $6 }' /etc/passwd | while read -r dir; do
    if [ -d "$dir" ]; then
        file="$dir/.rhosts"
        [ ! -h "$file" ] && [ -f "$file" ] && rm -f "$file"
    fi
done
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.			

6.2.18 Ensure there are no unnecessary accounts (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 Authorizing Official.

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, refer to the remediation procedure below.

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.

To remove the user, the user's home directory and the users mail spool

```
# userdel -r user's username
```

Document all authorized accounts on the system.

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204460
Rule ID: SV-204460r603261_rule
STIG ID: RHEL-07-020270
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

6.2.19 Ensure all local interactive user home directories are group-owned (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that all local interactive user home directories are group-owned by the home directory owners 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.

Check the home directory assignment for all local interactive users on the system with the following command:

```
# ls -ld $(egrep ':[0-9]{4}' /etc/passwd | cut -d: -f6)
-rwxr-x--- 1 smithj users 18 Mar 5 17:06 /home/smithj
```

Check the user's primary group with the following command:

```
# grep users /etc/group
users:x:250:smithj,jonesj,jacksons
```

If the local interactive users home directory referenced in `/etc/passwd` is not group-owned by that user's primary GID, refer to the remediation procedure below.

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. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204470
Rule ID: SV-204470r744102_rule
STIG ID: RHEL-07-020650
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

6.2.20 Ensure that all files and directories contained in local interactive user home directories are owned by the user (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 owned by the user of the home directory.

Rationale:

If local interactive users do not own the files in their directories, unauthorized users may be able to access them. Additionally, if files are not owned by the user, this could be an indication of system compromise.

Audit:

Verify all files and directories in a local interactive user's home directory are owned by the user.

Check the 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/smithj
-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 smithj 231 Mar 5 17:06 file3
```

If any files are found with an owner different than the home directory user, refer to the remediation procedure below.

Remediation:

Change the owner of a local interactive user's files and directories to that owner. To change the 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`.

```
# chown smithj /home/smithj/<file or directory>
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204471
Rule ID: SV-204471r744105_rule
STIG ID: RHEL-07-020660
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

6.2.21 Ensure local interactive user is a member of the group owner. (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 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 are found with an owner different than the group home directory user, 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 the user is not a member of a group that group owns file(s) in a local interactive user's home directory, refer to the remediation procedure below.

Remediation:

Change the group of a local interactive user's files and directories to a group that the interactive user is a member of. 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 users /home/smithj/<file>
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204472
Rule ID: SV-204472r603261_rule
STIG ID: RHEL-07-020670
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

6.2.22 Ensure users' files and directories within the home directory permissions are 750 or more restrictive (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that all files and directories contained in local interactive user home directories have a mode of 0750 or less permissive.

Rationale:

If a local interactive user files have excessive permissions, unintended users may be able to access or modify them.

Audit:

Verify all files and directories contained in a local interactive user home directory, excluding local initialization files, have a mode of 0750.

Check the mode of all non-initialization files in a local interactive user home directory with the following command:

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 are found with a mode more permissive than 0750, refer to the remediation procedure below.

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>
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204473
Rule ID: SV-204473r603261_rule
STIG ID: RHEL-07-020680
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

6.2.23 Ensure local interactive users' dot files for are owned by the user or root. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that all local initialization (dot) files for interactive users are owned by the home directory user or root.

Rationale:

Local initialization (dot) files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon login.

Audit:

Verify all local initialization files for interactive users are owned by the `home directory user` OR `root`.

Check the owner on all local initialization files 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 .bash_profile
-rwxr-xr-x 1 smithj users 497 Jan 6 2007 .login
-rwxr-xr-x 1 smithj users 886 Jan 6 2007 .profile
```

If any file that sets a local interactive user's environment variables to override the system is not owned by the `home directory owner` or `root`, refer to the remediation procedure below.

Remediation:

Set the owner of the local initialization files for interactive users to either the `home directory owner` or `root` with the following command:

Note: The example will be for the `smithj` user, who has a home directory of `/home/smithj`.

```
# chown smithj /home/smithj/. *
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204474
Rule ID: SV-204474r603834_rule
STIG ID: RHEL-07-020690
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	14.6 <u>Protect Information through Access Control Lists</u> 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.			

6.2.24 Ensure local interactive users' dot files are group-owned by the users group or root. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that all local initialization (`dot`) files for local interactive users are group-owned by the `users` primary group or `root`.

Rationale:

Local initialization (`dot`) files for interactive users are used to configure the user's shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Audit:

Verify the local initialization files of all local interactive users are group-owned by that user's primary Group Identifier (`GID`).

Check the home directory assignment for all non-privileged users on the system with the following command:

Note: The example will be for the `smithj` user, who has a home directory of `/home/smithj` and a primary group of `users`.

```
# cut -d: -f 1,4,6 /etc/passwd | egrep ":[1-4][0-9]{3}"  
  
smithj:1000:/home/smithj  
# grep 1000 /etc/group  
  
users:x:1000:smithj,jonesj,jacksons
```

Note: This may miss interactive users that have been assigned a privileged User Identifier (`UID`). Evidence of interactive use may be obtained from a number of log files containing system logon information.

Check the group owner of all local interactive user's initialization files with the following command:

```
# ls -al /home/smithj/.*  
-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 all local interactive user's initialization files are not group-owned by that user's primary GID, refer to the remediation procedure below.

Remediation:

Change the group owner of a local interactive user's files to the group found in `/etc/passwd` for the user. 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/<file>
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

```
Red Hat Enterprise Linux 7 Security Technical Implementation Guide  
Version 3, Release: 4 Benchmark Date: 23 Jul 2021  
  
Vul ID: V-204475  
Rule ID: SV-204475r603836_rule  
STIG ID: RHEL-07-020700  
Severity: CAT II
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>14.6 Protect Information through Access Control Lists</u> 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.			

6.2.25 Ensure users' dot files have 0740 or less set. (Automated)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that all local initialization (dot) files have mode 0740 or less permissive.

Rationale:

Local initialization (dot) 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.

Check the mode on all local initialization files 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----- 1 smithj users 896 Mar 10 2011 .profile
-rwxr----- 1 smithj users 497 Jan 6 2007 .login
-rwxr----- 1 smithj users 886 Jan 6 2007 .something
```

If any local initialization files have a mode more permissive than 0740, refer to the remediation procedure below.

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 0740 /home/smithj/.<INIT_FILE>
```

References:

1. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204476
Rule ID: SV-204476r603261_rule
STIG ID: RHEL-07-020710
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>14.6 Protect Information through Access Control Lists</u> 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.			

6.2.26 Ensure local interactive users' dot files executable paths resolve to the users home directory. (Manual)

Profile Applicability:

- STIG

Description:

The operating system must be configured so that all local interactive user initialization (dot) files executable search paths contain only paths that resolve to 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 files' (dot) executable search path statements do not contain statements that will reference a working directory other than the users' home directory.

Check the executable search path statement for all local interactive user initialization files in the users' home directory with the following commands:

Note: The example will be for the `smithj` user, which has a home directory of `/home/smithj`.

```
# grep -i path /home/smithj/.*

/home/smithj/.bash_profile:PATH=$PATH:$HOME/.local/bin:$HOME/bin
/home/smithj/.bash_profile:export PATH
```

If any local interactive user initialization files have executable search path statements that include directories outside of their home directory, refer to the remediation procedure below.

Remediation:

Edit the local interactive user initialization files to change any PATH variable statements that reference directories other than their home directory.

Note: The example will be for the `smithj` user, which has a home directory of

`/home/smithj`.

Utilizing the files listed in the Audit run this command to edit them and change the PATH variable statement.

Example: `vim /home/smithj/.bash_profile`

Update the PATH accordingly:

```
:PATH=$PATH:$HOME/.local/bin:$HOME/bin
```

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. CCI: CCI-000366: The organization implements the security configuration settings.
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

Additional Information:

Red Hat Enterprise Linux 7 Security Technical Implementation Guide
Version 3, Release: 4 Benchmark Date: 23 Jul 2021

Vul ID: V-204477
Rule ID: SV-204477r603261_rule
STIG ID: RHEL-07-020720
Severity: CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 Configure Data Access Control Lists</u> 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	<u>14.6 Protect Information through Access Control Lists</u> 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.			

Appendix: Recommendation Summary Table

Control		Set Correctly	
		Yes	No
1	Initial Setup		
1.1	Filesystem Configuration		
1.1.1	Disable unused filesystems		
1.1.1.1	Ensure mounting of cramfs filesystems is disabled (Automated)	☐	☐
1.1.1.2	Ensure mounting of squashfs filesystems is disabled (Automated)	☐	☐
1.1.1.3	Ensure mounting of udf filesystems is disabled (Automated)	☐	☐
1.1.2	Ensure /tmp is configured (Automated)	☐	☐
1.1.3	Ensure noexec option set on /tmp partition (Automated)	☐	☐
1.1.4	Ensure nodev option set on /tmp partition (Automated)	☐	☐
1.1.5	Ensure nosuid option set on /tmp partition (Automated)	☐	☐
1.1.6	Ensure /dev/shm is configured (Automated)	☐	☐
1.1.7	Ensure noexec option set on /dev/shm partition (Automated)	☐	☐
1.1.8	Ensure nodev option set on /dev/shm partition (Automated)	☐	☐
1.1.9	Ensure nosuid option set on /dev/shm partition (Automated)	☐	☐
1.1.10	Ensure separate partition exists for /var (Automated)	☐	☐
1.1.11	Ensure separate partition exists for /var/tmp (Automated)	☐	☐
1.1.12	Ensure /var/tmp partition includes the noexec option (Automated)	☐	☐
1.1.13	Ensure /var/tmp partition includes the nodev option (Automated)	☐	☐
1.1.14	Ensure /var/tmp partition includes the nosuid option (Automated)	☐	☐
1.1.15	Ensure separate partition exists for /var/log (Automated)	☐	☐
1.1.16	Ensure separate partition exists for /var/log/audit (Automated)	☐	☐
1.1.17	Ensure separate partition exists for /home (Automated)	☐	☐
1.1.18	Ensure /home partition includes the nodev option (Automated)	☐	☐
1.1.19	Ensure nosuid is set on users' home directories. (Automated)	☐	☐

1.1.20	Ensure removable media partitions include noexec option (Automated)	☐	☐
1.1.21	Ensure nodev option set on removable media partitions (Automated)	☐	☐
1.1.22	Ensure nosuid option set on removable media partitions (Automated)	☐	☐
1.1.23	Ensure noexec option is configured for NFS. (Automated)	☐	☐
1.1.24	Ensure nosuid option is set for NFS (Automated)	☐	☐
1.1.25	Ensure sticky bit is set on all world-writable directories (Automated)	☐	☐
1.1.26	Ensure all world-writable directories are group-owned. (Automated)	☐	☐
1.1.27	Disable Automounting (Automated)	☐	☐
1.1.28	Disable USB Storage (Automated)	☐	☐
1.2	Configure Software Updates		
1.2.1	Ensure GPG keys are configured (Manual)	☐	☐
1.2.2	Ensure package manager repositories are configured (Manual)	☐	☐
1.2.3	Ensure gpgcheck is globally activated (Automated)	☐	☐
1.2.4	Ensure software packages have been digitally signed by a Certificate Authority (CA) (Automated)	☐	☐
1.2.5	Ensure removal of software components after update (Automated)	☐	☐
1.2.6	Ensure the version of the operating system is an active vendor supported release (Manual)	☐	☐
1.3	Filesystem Integrity Checking		
1.3.1	Ensure AIDE is installed (Automated)	☐	☐
1.3.2	Ensure filesystem integrity is regularly checked (Automated)	☐	☐
1.3.3	Ensure AIDE is configured to verify ACLs (Manual)	☐	☐
1.3.4	Ensure AIDE is configured to verify XATTRS (Manual)	☐	☐
1.3.5	Ensure AIDE is configured to use FIPS 140-2 (Manual)	☐	☐
1.4	Secure Boot Settings		
1.4.1	Ensure bootloader password is set (Automated)	☐	☐
1.4.2	Ensure permissions on bootloader config are configured (Automated)	☐	☐
1.4.3	Ensure authentication required for single user mode (Automated)	☐	☐
1.4.4	Ensure boot loader does not allow removable media (Automated)	☐	☐
1.4.5	Ensure version 7.2 or newer booted with a BIOS have a unique name for the grub superusers account (Manual)	☐	☐

1.4.6	Ensure version 7.2 or newer booted with UEFI have a unique name for the grub superusers account (Manual)	☐	☐
1.5	Additional Process Hardening		
1.5.1	Ensure core dumps are restricted (Automated)	☐	☐
1.5.2	Ensure XD/NX support is enabled (Automated)	☐	☐
1.5.3	Ensure address space layout randomization (ASLR) is enabled (Automated)	☐	☐
1.5.4	Ensure prelink is not installed (Automated)	☐	☐
1.5.5	Ensure number of concurrent sessions is limited (Automated)	☐	☐
1.5.6	Ensure the Ctrl-Alt-Delete key sequence is disabled. (Automated)	☐	☐
1.5.7	Ensure kernel core dumps are disabled. (Automated)	☐	☐
1.5.8	Ensure DNS servers are configured (Automated)	☐	☐
1.5.9	Ensure NIST FIPS-validated cryptography is configured (Automated)	☐	☐
1.6	Mandatory Access Control		
1.6.1	Configure SELinux		
1.6.1.1	Ensure SELinux is installed (Automated)	☐	☐
1.6.1.2	Ensure SELinux is not disabled in bootloader configuration (Automated)	☐	☐
1.6.1.3	Ensure SELinux policy is configured (Automated)	☐	☐
1.6.1.4	Ensure the SELinux mode is enforcing or permissive (Automated)	☐	☐
1.6.1.5	Ensure the SELinux mode is enforcing (Automated)	☐	☐
1.6.1.6	Ensure no unconfined services exist (Automated)	☐	☐
1.6.1.7	Ensure SETroubleshoot is not installed (Automated)	☐	☐
1.6.1.8	Ensure the MCS Translation Service (mcstrans) is not installed (Automated)	☐	☐
1.6.1.9	Ensure non-privileged users are prevented from executing privileged functions (Manual)	☐	☐
1.6.1.10	Ensure system device files are labeled. (Manual)	☐	☐
1.7	Command Line Warning Banners		
1.7.1	Ensure message of the day is configured properly (Automated)	☐	☐
1.7.2	Ensure local login warning banner is configured properly (Automated)	☐	☐
1.7.3	Ensure the Standard Mandatory DoD Notice and Consent Banner are configured (Automated)	☐	☐
1.7.4	Ensure remote login warning banner is configured properly (Automated)	☐	☐
1.7.5	Ensure permissions on /etc/motd are configured (Automated)	☐	☐

1.7.6	Ensure permissions on /etc/issue are configured (Automated)	☐	☐
1.7.7	Ensure permissions on /etc/issue.net are configured (Automated)	☐	☐
1.7.8	Ensure the Standard Mandatory DoD Notice and Consent Banner are configured (Manual)	☐	☐
1.8	GNOME Display Manager		
1.8.1	Ensure GDM login banner is configured (Manual)	☐	☐
1.8.2	Ensure Standard Mandatory DoD Notice and Consent Banner displayed via a graphical user logon (Manual)	☐	☐
1.8.3	Ensure GDM session lock is enabled (Automated)	☐	☐
1.8.4	Ensure the graphical user Ctrl-Alt-Delete key sequence is disabled (Automated)	☐	☐
1.8.5	Ensure users must authenticate users using MFA via a graphical user logon (Automated)	☐	☐
1.8.6	Ensure GNOME Screensaver period of inactivity is configured (Automated)	☐	☐
1.8.7	Ensure screensaver lock-enabled is set (Automated)	☐	☐
1.8.8	Ensure overriding the screensaver lock-delay setting is prevented (Automated)	☐	☐
1.8.9	Ensure session idle-delay settings is enforced (Automated)	☐	☐
1.8.10	Ensure GNOME Idle activation is set (Automated)	☐	☐
1.8.11	Ensure the screensaver idle-activation-enabled setting (Automated)	☐	☐
1.8.12	Ensure GNOME Lock Delay is configured (Automated)	☐	☐
1.8.13	Ensure automatic logon via GUI is not allowed (Automated)	☐	☐
1.8.14	Ensure unrestricted logon is not allowed (Automated)	☐	☐
1.8.15	Ensure graphical user interface automounter is disabled (Automated)	☐	☐
1.9	Ensure updates, patches, and additional security software are installed (Manual)	☐	☐
1.10	Ensure required packages for multifactor authentication are installed (Automated)	☐	☐
1.11	Ensure anti-virus is installed and running (Manual)	☐	☐
1.12	Ensure host-based intrusion detection tool is used (Manual)	☐	☐
2	Services		
2.1	inetd Services		
2.1.1	Ensure xinetd is not installed (Automated)	☐	☐
2.2	Special Purpose Services		
2.2.1	Time Synchronization		
2.2.1.1	Ensure time synchronization is in use (Manual)	☐	☐
2.2.1.2	Ensure chrony is configured (Automated)	☐	☐
2.2.1.3	Ensure ntp is configured (Automated)	☐	☐

2.2.1.4	Ensure internal information system clocks are synchronizing (Automated)	☐	☐
2.2.2	Ensure X11 Server components are not installed (Automated)	☐	☐
2.2.3	Ensure Avahi Server is not installed (Automated)	☐	☐
2.2.4	Ensure CUPS is not installed (Automated)	☐	☐
2.2.5	Ensure DHCP Server is not installed (Automated)	☐	☐
2.2.6	Ensure LDAP server is not installed (Automated)	☐	☐
2.2.7	Ensure DNS Server is not installed (Automated)	☐	☐
2.2.8	Ensure FTP Server is not installed (Automated)	☐	☐
2.2.9	Ensure HTTP server is not installed (Automated)	☐	☐
2.2.10	Ensure IMAP and POP3 server is not installed (Automated)	☐	☐
2.2.11	Ensure Samba is not installed (Automated)	☐	☐
2.2.12	Ensure HTTP Proxy Server is not installed (Automated)	☐	☐
2.2.13	Ensure net-snmp is not installed (Automated)	☐	☐
2.2.14	Ensure NIS server is not installed (Automated)	☐	☐
2.2.15	Ensure telnet-server is not installed (Automated)	☐	☐
2.2.16	Ensure mail transfer agent is configured for local-only mode (Automated)	☐	☐
2.2.17	Ensure nfs-utils is not installed or the nfs-server service is masked (Automated)	☐	☐
2.2.18	Ensure rpcbind is not installed or the rpcbind services are masked (Automated)	☐	☐
2.2.19	Ensure rsync is not installed or the rsyncd service is masked (Automated)	☐	☐
2.2.20	Ensure the rsh package has been removed (Automated)	☐	☐
2.2.21	Ensure the TFTP server has not been installed (Automated)	☐	☐
2.2.22	Ensure TFTP daemon is configured to operate in secure mode (Automated)	☐	☐
2.2.23	Ensure default SNMP community strings don't exist (Automated)	☐	☐
2.2.24	Ensure NFS is configured to use RPCSEC_GSS (Automated)	☐	☐
2.2.25	Ensure unrestricted mail relaying is prevented (Automated)	☐	☐
2.2.26	Ensure ldap_tls_cacert is set for LDAP. (Automated)	☐	☐
2.2.27	Ensure ldap_id_use_start_tls is set for LDAP. (Automated)	☐	☐
2.2.28	Ensure ldap_tls_reqcert is set for LDAP (Automated)	☐	☐
2.3	Service Clients		
2.3.1	Ensure NIS Client is not installed (Automated)	☐	☐
2.3.2	Ensure rsh client is not installed (Automated)	☐	☐
2.3.3	Ensure talk client is not installed (Automated)	☐	☐
2.3.4	Ensure telnet client is not installed (Automated)	☐	☐
2.3.5	Ensure LDAP client is not installed (Automated)	☐	☐

2.4	Ensure nonessential services are removed or masked (Manual)	☐	☐
3	Network Configuration		
3.1	Disable unused network protocols and devices		
3.1.1	Disable IPv6 (Manual)	☐	☐
3.1.2	Ensure wireless interfaces are disabled (Automated)	☐	☐
3.2	Network Parameters (Host Only)		
3.2.1	Ensure IP forwarding is disabled (Automated)	☐	☐
3.2.2	Ensure packet redirect sending is disabled (Automated)	☐	☐
3.3	Network Parameters (Host and Router)		
3.3.1	Ensure source routed packets are not accepted (Automated)	☐	☐
3.3.2	Ensure ICMP redirects are not accepted (Automated)	☐	☐
3.3.3	Ensure network interfaces are not in promiscuous mode (Manual)	☐	☐
3.3.4	Ensure secure ICMP redirects are not accepted (Automated)	☐	☐
3.3.5	Ensure suspicious packets are logged (Automated)	☐	☐
3.3.6	Ensure broadcast ICMP requests are ignored (Automated)	☐	☐
3.3.7	Ensure bogus ICMP responses are ignored (Automated)	☐	☐
3.3.8	Ensure Reverse Path Filtering is enabled (Automated)	☐	☐
3.3.9	Ensure TCP SYN Cookies is enabled (Automated)	☐	☐
3.3.10	Ensure IPv6 router advertisements are not accepted (Automated)	☐	☐
3.4	Uncommon Network Protocols		
3.4.1	Ensure DCCP is disabled (Automated)	☐	☐
3.4.2	Ensure SCTP is disabled (Automated)	☐	☐
3.5	Firewall Configuration		
3.5.1	Configure firewalld		
3.5.1.1	Ensure firewalld is installed (Automated)	☐	☐
3.5.1.2	Ensure iptables-services not installed with firewalld (Automated)	☐	☐
3.5.1.3	Ensure nftables either not installed or masked with firewalld (Automated)	☐	☐
3.5.1.4	Ensure firewalld service enabled and running (Automated)	☐	☐
3.5.1.5	Ensure firewalld default zone is set (Automated)	☐	☐
3.5.1.6	Ensure network interfaces are assigned to appropriate zone (Manual)	☐	☐
3.5.1.7	Ensure firewalld drops unnecessary services and ports (Manual)	☐	☐
3.5.2	Configure nftables		
3.5.2.1	Ensure nftables is installed (Automated)	☐	☐
3.5.2.2	Ensure firewalld is either not installed or masked with nftables (Automated)	☐	☐

3.5.2.3	Ensure iptables-services not installed with nftables (Automated)	☐	☐
3.5.2.4	Ensure iptables are flushed with nftables (Manual)	☐	☐
3.5.2.5	Ensure an nftables table exists (Automated)	☐	☐
3.5.2.6	Ensure nftables base chains exist (Automated)	☐	☐
3.5.2.7	Ensure nftables loopback traffic is configured (Automated)	☐	☐
3.5.2.8	Ensure nftables outbound and established connections are configured (Manual)	☐	☐
3.5.2.9	Ensure nftables default deny firewall policy (Automated)	☐	☐
3.5.2.10	Ensure nftables service is enabled (Automated)	☐	☐
3.5.2.11	Ensure nftables rules are permanent (Automated)	☐	☐
3.5.3	Configure iptables		
3.5.3.1	Configure iptables software		
3.5.3.1.1	Ensure iptables packages are installed (Automated)	☐	☐
3.5.3.1.2	Ensure nftables is not installed with iptables (Automated)	☐	☐
3.5.3.1.3	Ensure firewalld is either not installed or masked with iptables (Automated)	☐	☐
3.5.3.2	Configure IPv4 iptables		
3.5.3.2.1	Ensure iptables loopback traffic is configured (Automated)	☐	☐
3.5.3.2.2	Ensure iptables outbound and established connections are configured (Manual)	☐	☐
3.5.3.2.3	Ensure iptables rules exist for all open ports (Automated)	☐	☐
3.5.3.2.4	Ensure iptables default deny firewall policy (Automated)	☐	☐
3.5.3.2.5	Ensure iptables rules are saved (Automated)	☐	☐
3.5.3.2.6	Ensure iptables is enabled and running (Automated)	☐	☐
3.5.3.3	Configure IPv6 ip6tables		
3.5.3.3.1	Ensure ip6tables loopback traffic is configured (Automated)	☐	☐
3.5.3.3.2	Ensure ip6tables outbound and established connections are configured (Manual)	☐	☐
3.5.3.3.3	Ensure ip6tables firewall rules exist for all open ports (Automated)	☐	☐
3.5.3.3.4	Ensure ip6tables default deny firewall policy (Automated)	☐	☐
3.5.3.3.5	Ensure ip6tables rules are saved (Automated)	☐	☐
3.5.3.3.6	Ensure ip6tables is enabled and running (Automated)	☐	☐
3.5.4	Ensure IP tunnels are not configured (Automated)	☐	☐
4	Logging and Auditing		
4.1	Configure System Accounting (auditd)		
4.1.1	Ensure auditing is enabled		
4.1.1.1	Ensure auditd is installed (Automated)	☐	☐
4.1.1.2	Ensure auditd service is enabled and running (Automated)	☐	☐
4.1.1.3	Ensure auditing for processes that start prior to auditd is enabled (Automated)	☐	☐
4.1.2	Configure Data Retention		

4.1.2.1	Ensure audit log storage size is configured (Automated)	☐	☐
4.1.2.2	Ensure audit logs are not automatically deleted (Automated)	☐	☐
4.1.2.3	Ensure audit system is set to single when the disk is full. (Automated)	☐	☐
4.1.2.4	Ensure system notification is sent out when volume is 75% full (Manual)	☐	☐
4.1.2.5	Ensure system is disabled when audit logs are full (Automated)	☐	☐
4.1.2.6	Ensure audit system action is defined for sending errors (Automated)	☐	☐
4.1.2.7	Ensure audit_backlog_limit is sufficient (Automated)	☐	☐
4.1.2.8	Ensure audit logs are stored on a different system. (Manual)	☐	☐
4.1.2.9	Ensure audit logs on separate system are encrypted. (Automated)	☐	☐
4.1.2.10	Ensure the auditing processing failures are handled. (Automated)	☐	☐
4.1.2.11	Ensure off-load of audit logs. (Automated)	☐	☐
4.1.2.12	Ensure action is taken when audisp-remote buffer is full (Automated)	☐	☐
4.1.2.13	Ensure off-loaded audit logs are labeled. (Automated)	☐	☐
4.1.3	Configure auditd rules		
4.1.3.1	Ensure events that modify date and time information are collected (Automated)	☐	☐
4.1.3.2	Ensure system administrator command executions (sudo) are collected (Automated)	☐	☐
4.1.3.3	Ensure session initiation information is collected (Automated)	☐	☐
4.1.3.4	Ensure events that modify the system's Mandatory Access Controls are collected (Automated)	☐	☐
4.1.3.5	Ensure events that modify the system's network environment are collected (Automated)	☐	☐
4.1.3.6	Ensure successful file system mounts are collected (Automated)	☐	☐
4.1.3.7	Ensure kernel module loading and unloading is collected (Automated)	☐	☐
4.1.3.8	Ensure changes to system administration scope (sudoers) is collected (Automated)	☐	☐
4.1.3.9	Ensure file deletion events by users are collected (Automated)	☐	☐
4.1.3.10	Ensure use of privileged commands is collected (Automated)	☐	☐
4.1.3.11	Ensure unsuccessful unauthorized file access attempts are collected (Automated)	☐	☐

4.1.3.12	Ensure discretionary access control permission modification events are collected (Automated)	☐	☐
4.1.3.13	Ensure login and logout events are collected (Automated)	☐	☐
4.1.3.14	Ensure events that modify user/group information are collected (Automated)	☐	☐
4.1.3.15	Ensure all uses of the passwd command are audited. (Automated)	☐	☐
4.1.3.16	Ensure auditing of the unix_chkpwd command (Automated)	☐	☐
4.1.3.17	Ensure audit of the gpasswd command (Automated)	☐	☐
4.1.3.18	Ensure audit all uses of chage (Automated)	☐	☐
4.1.3.19	Ensure audit all uses of the chsh command. (Automated)	☐	☐
4.1.3.20	Ensure audit the umount command (Automated)	☐	☐
4.1.3.21	Ensure audit of postdrop command (Automated)	☐	☐
4.1.3.22	Ensure audit of postqueue command. (Automated)	☐	☐
4.1.3.23	Ensure audit ssh-keysign command. (Automated)	☐	☐
4.1.3.24	Ensure audit of crontab command (Automated)	☐	☐
4.1.3.25	Ensure audit of kmod command (Automated)	☐	☐
4.1.3.26	Ensure audit of the rmdir syscall (Automated)	☐	☐
4.1.3.27	Ensure audit of unlink syscall (Automated)	☐	☐
4.1.3.28	Ensure audit unlinkat syscall (Automated)	☐	☐
4.1.3.29	Ensure audit pam_timestamp_check command (Automated)	☐	☐
4.1.3.30	Ensure audit of the finit_module syscall (Automated)	☐	☐
4.1.3.31	Ensure audit of the create_module syscall (Automated)	☐	☐
4.1.3.32	Ensure auditing of all privileged functions (Automated)	☐	☐
4.1.3.33	Ensure audit of semanage command (Automated)	☐	☐
4.1.3.34	Ensure audit of the setsebool command. (Automated)	☐	☐
4.1.3.35	Ensure audit of the chcon command (Automated)	☐	☐
4.1.3.36	Ensure audit of the userhelper command (Automated)	☐	☐
4.1.3.37	Ensure audit of the mount command and syscall (Automated)	☐	☐
4.1.3.38	Ensure audit of the su command (Automated)	☐	☐
4.1.3.39	Ensure audit of setfiles command (Automated)	☐	☐
4.1.3.40	Ensure audit all uses of the newgrp command (Automated)	☐	☐
4.1.3.41	Ensure the audit configuration is immutable (Automated)	☐	☐
4.1.4	Configure auditd file access		
4.1.4.1	Ensure Audit logs are owned by root and mode 0600 or less permissive (Automated)	☐	☐
4.2	Configure Logging		
4.2.1	Configure rsyslog		
4.2.1.1	Ensure rsyslog is installed (Automated)	☐	☐
4.2.1.2	Ensure rsyslog Service is enabled and running (Automated)	☐	☐
4.2.1.3	Ensure rsyslog default file permissions configured (Automated)	☐	☐

4.2.1.4	Ensure logging is configured (Manual)	☐	☐
4.2.1.5	Ensure rsyslog is configured to send logs to a remote log host (Automated)	☐	☐
4.2.1.6	Ensure remote rsyslog messages are only accepted on designated log hosts. (Manual)	☐	☐
4.2.2	Configure journald		
4.2.2.1	Ensure journald is configured to send logs to rsyslog (Automated)	☐	☐
4.2.2.2	Ensure journald is configured to compress large log files (Automated)	☐	☐
4.2.2.3	Ensure journald is configured to write logfiles to persistent disk (Automated)	☐	☐
4.2.3	Ensure logrotate is configured (Manual)	☐	☐
4.2.4	Ensure permissions on all logfiles are configured (Manual)	☐	☐
5	Access, Authentication and Authorization		
5.1	Configure time-based job schedulers		
5.1.1	Ensure cron daemon is enabled and running (Automated)	☐	☐
5.1.2	Ensure permissions on /etc/crontab are configured (Automated)	☐	☐
5.1.3	Ensure permissions on /etc/cron.hourly are configured (Automated)	☐	☐
5.1.4	Ensure permissions on /etc/cron.daily are configured (Automated)	☐	☐
5.1.5	Ensure permissions on /etc/cron.weekly are configured (Automated)	☐	☐
5.1.6	Ensure permissions on /etc/cron.monthly are configured (Automated)	☐	☐
5.1.7	Ensure permissions on /etc/cron.d are configured (Automated)	☐	☐
5.1.8	Ensure cron is restricted to authorized users (Automated)	☐	☐
5.1.9	Ensure at is restricted to authorized users (Automated)	☐	☐
5.2	Configure sudo		
5.2.1	Ensure sudo is installed (Automated)	☐	☐
5.2.2	Ensure sudo commands use pty (Automated)	☐	☐
5.2.3	Ensure sudo log file exists (Automated)	☐	☐
5.2.4	Ensure users must provide password for escalation (Automated)	☐	☐
5.2.5	Ensure users must re-authenticate for privilege escalation (Automated)	☐	☐
5.2.6	Ensure the sudoers file restricts sudo access to authorized personnel (Automated)	☐	☐
5.2.7	Ensure sudo authentication timeout is configured (Automated)	☐	☐

5.2.8	Ensure users password required for privilege escalation when using sudo (Automated)	☐	☐
5.3	Configure SSH Server		
5.3.1	Ensure SSH is installed (Automated)	☐	☐
5.3.2	Ensure SSH is running (Automated)	☐	☐
5.3.3	Ensure permissions on /etc/ssh/sshd_config are configured (Automated)	☐	☐
5.3.4	Ensure permissions on SSH private host key files are configured (Automated)	☐	☐
5.3.5	Ensure permissions on SSH public host key files are configured (Automated)	☐	☐
5.3.6	Ensure SSH access is limited (Automated)	☐	☐
5.3.7	Ensure SSH LogLevel is appropriate (Automated)	☐	☐
5.3.8	Ensure SSH X11 forwarding is disabled (Automated)	☐	☐
5.3.9	Ensure SSH MaxAuthTries is set to 4 or less (Automated)	☐	☐
5.3.10	Ensure SSH IgnoreRhosts is enabled (Automated)	☐	☐
5.3.11	Ensure SSH HostbasedAuthentication is disabled (Automated)	☐	☐
5.3.12	Ensure SSH root login is disabled (Automated)	☐	☐
5.3.13	Ensure SSH PermitEmptyPasswords is disabled (Automated)	☐	☐
5.3.14	Ensure SSH PermitUserEnvironment is disabled (Automated)	☐	☐
5.3.15	Ensure only strong Ciphers are used (Automated)	☐	☐
5.3.16	Ensure only FIPS 140-2 ciphers are used for SSH (Automated)	☐	☐
5.3.17	Ensure only strong MAC algorithms are used (Automated)	☐	☐
5.3.18	Ensure only strong Key Exchange algorithms are used (Automated)	☐	☐
5.3.19	Ensure SSH Idle Timeout Interval is configured (Automated)	☐	☐
5.3.20	Ensure SSH LoginGraceTime is set to one minute or less (Automated)	☐	☐
5.3.21	Ensure SSH warning banner is configured (Automated)	☐	☐
5.3.22	Ensure SSH PAM is enabled (Automated)	☐	☐
5.3.23	Ensure SSH AllowTcpForwarding is disabled (Automated)	☐	☐
5.3.24	Ensure SSH MaxStartups is configured (Automated)	☐	☐
5.3.25	Ensure SSH MaxSessions is limited (Automated)	☐	☐
5.3.26	Ensure RSA rhosts authentication is not allowed (Automated)	☐	☐
5.3.27	Ensure Printlastlog is enabled (Automated)	☐	☐
5.3.28	Ensure SSH IgnoreUserKnownHosts is enabled (Automated)	☐	☐
5.3.29	Ensure SSH Protocol is set to 2 (Automated)	☐	☐
5.3.30	Ensure SSH does not permit GSSAPI (Automated)	☐	☐

5.3.31	Ensure SSH does not permit Kerberos authentication (Automated)	☐	☐
5.3.32	Ensure SSH performs checks of home directory configuration files (Automated)	☐	☐
5.3.33	Ensure SSH uses privilege separation (Automated)	☐	☐
5.3.34	Ensure SSH compressions setting is delayed (Automated)	☐	☐
5.3.35	Ensure SSH X11UseLocalhost is enabled (Automated)	☐	☐
5.3.36	Ensure no ".shosts" files exist on the system (Manual)	☐	☐
5.3.37	Ensure no "shosts.equiv" files exist on the system (Manual)	☐	☐
5.4	Configure PAM		
5.4.1	Ensure password creation requirements are configured (Automated)	☐	☐
5.4.2	Ensure lockout for failed password attempts is configured (Automated)	☐	☐
5.4.3	Ensure password hashing algorithm is SHA-512 (Automated)	☐	☐
5.4.4	Ensure password reuse is limited (Automated)	☐	☐
5.4.5	Ensure system-auth is used when changing passwords (Automated)	☐	☐
5.4.6	Ensure no accounts are configured with blank or null passwords (Automated)	☐	☐
5.4.7	Ensure minimum and maximum requirements are set for password changes (Automated)	☐	☐
5.4.8	Ensure date and time of last successful logon (Automated)	☐	☐
5.4.9	Ensure multifactor authentication for access to privileged accounts (Automated)	☐	☐
5.4.10	Ensure certificate status checking for PKI authentication (Automated)	☐	☐
5.4.11	Ensure password prohibited reuse is at a minimum 5 (Automated)	☐	☐
5.4.12	Ensure accounts lock for a minimum of 15 minutes after three unsuccessful logon attempts within a 15-minute timeframe (Automated)	☐	☐
5.4.13	Ensure lockout for unsuccessful root logon attempts (Automated)	☐	☐
5.5	User Accounts and Environment		
5.5.1	Set Shadow Password Suite Parameters		
5.5.1.1	Ensure password expiration is 365 days or less (Automated)	☐	☐
5.5.1.2	Ensure minimum days between password changes is configured (Automated)	☐	☐
5.5.1.3	Ensure password expiration warning days is 7 or more (Automated)	☐	☐
5.5.1.4	Ensure inactive password lock is 30 days or less (Automated)	☐	☐

5.5.1.5	Ensure all users last password change date is in the past (Automated)	☐	☐
5.5.1.6	Ensure shadow file is configured to use only encrypted representations of passwords (Automated)	☐	☐
5.5.1.7	Ensure password expiration is 60 Day maximum for new users (Automated)	☐	☐
5.5.1.8	Ensure password expiration is 60 Day maximum for existing passwords (Automated)	☐	☐
5.5.1.9	Ensure inactive password lock is 0 days (Automated)	☐	☐
5.5.1.10	Ensure delay between logon prompts on failure (Automated)	☐	☐
5.5.2	Ensure system accounts are secured (Automated)	☐	☐
5.5.3	Ensure default group for the root account is GID 0 (Automated)	☐	☐
5.5.4	Ensure default user shell timeout is configured (Automated)	☐	☐
5.5.5	Ensure default user umask is configured (Automated)	☐	☐
5.5.6	Ensure user and group account administration utilities are configured to store only encrypted representations of passwords (Automated)	☐	☐
5.5.7	Ensure multi-factor authentication is enable for users (Automated)	☐	☐
5.5.8	Ensure Default user umask is 077 (Automated)	☐	☐
5.5.9	Ensure local interactive user accounts umask is 077 (Automated)	☐	☐
5.5.10	Ensure upon user creation a home directory is assigned. (Automated)	☐	☐
5.6	Ensure root login is restricted to system console (Manual)	☐	☐
5.7	Ensure access to the su command is restricted (Automated)	☐	☐
6	System Maintenance		
6.1	System File Permissions		
6.1.1	Audit system file permissions (Manual)	☐	☐
6.1.2	Ensure permissions on /etc/passwd are configured (Automated)	☐	☐
6.1.3	Ensure permissions on /etc/passwd- are configured (Automated)	☐	☐
6.1.4	Ensure permissions on /etc/shadow are configured (Automated)	☐	☐
6.1.5	Ensure permissions on /etc/shadow- are configured (Automated)	☐	☐
6.1.6	Ensure permissions on /etc/gshadow- are configured (Automated)	☐	☐
6.1.7	Ensure permissions on /etc/gshadow are configured (Automated)	☐	☐

6.1.8	Ensure permissions on /etc/group are configured (Automated)	☐	☐
6.1.9	Ensure permissions on /etc/group- are configured (Automated)	☐	☐
6.1.10	Ensure no world writable files exist (Automated)	☐	☐
6.1.11	Ensure no unowned files or directories exist (Automated)	☐	☐
6.1.12	Ensure no ungrouped files or directories exist (Automated)	☐	☐
6.1.13	Audit SUID executables (Manual)	☐	☐
6.1.14	Audit SGID executables (Manual)	☐	☐
6.1.15	Ensure the file permissions ownership and group membership of system files and commands match the vendor values (Manual)	☐	☐
6.1.16	Ensure all world-writable directorys are owned by root, sys, bin, or an application User Identifier (Manual)	☐	☐
6.2	User and Group Settings		
6.2.1	Ensure accounts in /etc/passwd use shadowed passwords (Automated)	☐	☐
6.2.2	Ensure /etc/shadow password fields are not empty (Automated)	☐	☐
6.2.3	Ensure all groups in /etc/passwd exist in /etc/group (Automated)	☐	☐
6.2.4	Ensure shadow group is empty (Automated)	☐	☐
6.2.5	Ensure no duplicate user names exist (Automated)	☐	☐
6.2.6	Ensure no duplicate group names exist (Automated)	☐	☐
6.2.7	Ensure no duplicate UIDs exist (Automated)	☐	☐
6.2.8	Ensure no duplicate GIDs exist (Automated)	☐	☐
6.2.9	Ensure root is the only UID 0 account (Automated)	☐	☐
6.2.10	Ensure root PATH Integrity (Automated)	☐	☐
6.2.11	Ensure all users' home directories exist (Automated)	☐	☐
6.2.12	Ensure users own their home directories (Automated)	☐	☐
6.2.13	Ensure users' home directories permissions are 750 or more restrictive (Automated)	☐	☐
6.2.14	Ensure users' dot files are not group or world writable (Automated)	☐	☐
6.2.15	Ensure no users have .forward files (Automated)	☐	☐
6.2.16	Ensure no users have .netrc files (Automated)	☐	☐
6.2.17	Ensure no users have .rhosts files (Automated)	☐	☐
6.2.18	Ensure there are no unnecessary accounts (Manual)	☐	☐
6.2.19	Ensure all local interactive user home directories are group-owned (Automated)	☐	☐
6.2.20	Ensure that all files and directories contained in local interactive user home directories are owned by the user (Automated)	☐	☐

6.2.21	Ensure local interactive user is a member of the group owner. (Automated)	☐	☐
6.2.22	Ensure users' files and directories within the home directory permissions are 750 or more restrictive (Automated)	☐	☐
6.2.23	Ensure local interactive users' dot files for are owned by the user or root. (Automated)	☐	☐
6.2.24	Ensure local interactive users' dot files are group-owned by the users group or root. (Automated)	☐	☐
6.2.25	Ensure users' dot files have 0740 or less set. (Automated)	☐	☐
6.2.26	Ensure local interactive users' dot files executable paths resolve to the users home directory. (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Nov 10, 2021	2.0.0	DELETE – Extended profile – STIG
Nov 10, 2021	2.0.0	ADD – Independent profile - STIG
Nov 10, 2021	2.0.0	DELETE – Mapping to CIS Controls version 6
Nov 10, 2021	2.0.0	ADD – Mappings to CIS Controls version 8
Nov 10, 2021	2.0.0	DELETE – Mapping references to: Red Hat Enterprise Linux 7 Security Technical Implementation Guide: Version 2, Release: 3 Benchmark Date: 26 Apr 2019
Nov 10, 2021	2.0.0	ADD - Mapping references to: Red Hat Enterprise Linux 7 Security Technical Implementation Guide: Version 3, Release: 4 Benchmark Date: 23 Jul 2021
Nov 10, 2021	2.0.0	DELETE - Ensure mounting of freevxfs filesystems is disabled
Nov 10, 2021	2.0.0	DELETE - Ensure mounting of FAT filesystems is limited
Nov 10, 2021	2.0.0	DELETE - Ensure mounting of jffs2 filesystems is disabled
Nov 10, 2021	2.0.0	DELETE - Ensure mounting of hfs filesystems is disabled
Nov 10, 2021	2.0.0	DELETE - Ensure mounting of hfsplus filesystems is disabled
Nov 10, 2021	2.0.0	UPDATE - 1.1.1.2 Ensure mounting of squashfs filesystems is disabled Audit Procedure: command modified to correct possible output error
Nov 10, 2021	2.0.0	UPDATE - 1.1.1.3 Ensure mounting of udf filesystems is disabled Audit Procedure: command modified to correct possible output error
Nov 10, 2021	2.0.0	UPDATE - 1.1.2 Ensure /tmp is configured Audit Procedure: command updated Remediation Procedure: include tmp.mount file example and add steps for tmp.mount option
Nov 10, 2021	2.0.0	DELETE - Ensure separate file system for /tmp
Nov 10, 2021	2.0.0	UPDATE - 1.1.3 Ensure noexec option set on /tmp partition Audit Procedure: command updated Remediation Procedure: Add steps for tmp.mount option
Nov 10, 2021	2.0.0	ADD - 1.1.4 Ensure nodev option set on /tmp partition
Nov 10, 2021	2.0.0	UPDATE - 1.1.5 Ensure nosuid option set on /tmp partition Audit Procedure: command updated Remediation Procedure: Add steps for tmp.mount option
Nov 10, 2021	2.0.0	ADD - 1.1.6 Ensure /dev/shm is configured
Nov 10, 2021	2.0.0	UPDATE - 1.1.7 Ensure noexec option set on /dev/shm partition Audit Procedure: command updated

Nov 10, 2021	2.0.0	UPDATE - 1.1.8 Ensure nodev option set on /dev/shm partition Audit Procedure: command updated
Nov 10, 2021	2.0.0	UPDATE - 1.1.9 Ensure nosuid option set on /dev/shm partition Audit Procedure: command updated
Nov 10, 2021	2.0.0	UPDATE - 1.1.10 Ensure separate partition exists for /var Audit Procedure: command updated
Nov 10, 2021	2.0.0	UPDATE - 1.1.11 Ensure separate partition exists for /var/tmp Audit Procedure: command updated
Nov 10, 2021	2.0.0	DELETE - Ensure noexec option set on /var/tmp partition
Nov 10, 2021	2.0.0	ADD - 1.1.12 Ensure /var/tmp partition includes the noexec option
Nov 10, 2021	2.0.0	DELETE - Ensure nodev option set on /var/tmp partition
Nov 10, 2021	2.0.0	ADD - 1.1.13 Ensure /var/tmp partition includes the nodev option
Nov 10, 2021	2.0.0	DELETE - Ensure nosuid option set on /var/tmp partition
Nov 10, 2021	2.0.0	ADD - 1.1.14 Ensure /var/tmp partition includes the nosuid option
Nov 10, 2021	2.0.0	UPDATE - 1.1.15 Ensure separate partition exists for /var/log Audit Procedure: command updated
Nov 10, 2021	2.0.0	UPDATE - 1.1.16 Ensure separate partition exists for /var/log/audit Audit Procedure: command updated
Nov 10, 2021	2.0.0	UPDATE - 1.1.17 Ensure separate partition exists for /home Audit Procedure: command updated
Nov 10, 2021	2.0.0	DELETE - Ensure nodev option set on /home partition
Nov 10, 2021	2.0.0	ADD - 1.1.18 Ensure /home partition includes the nodev option
Nov 10, 2021	2.0.0	ADD - 1.1.19 Ensure nosuid is set on users' home directories
Nov 10, 2021	2.0.0	DELETE - Ensure noexec option set on removable media partitions
Nov 10, 2021	2.0.0	ADD - 1.1.20 Ensure removable media partitions include noexec option
Nov 10, 2021	2.0.0	DELETE - Ensure nodev option set on removable media partitions
Nov 10, 2021	2.0.0	ADD - 1.1.21 Ensure nodev option set on removable media partitions
Nov 10, 2021	2.0.0	DELETE - Ensure nosuid option set on removable media partitions
Nov 10, 2021	2.0.0	ADD - 1.1.22 Ensure nosuid option set on removable media partitions
Nov 10, 2021	2.0.0	DELETE - Ensure noexec option set on removable media partitions
Nov 10, 2021	2.0.0	ADD - 1.1.23 Ensure noexec option is configured for NFS
Nov 10, 2021	2.0.0	ADD - 1.1.24 Ensure nosuid option is set for NFS
Nov 10, 2021	2.0.0	UPDATE - 1.1.27 Disable Automounting Audit Procedure: update command used for audit Remediation Procedure: update commands being used for remediation

Nov 10, 2021	2.0.0	UPDATE - 1.2.3 Ensure gpgcheck is globally activated Audit Procedure: update command used for audit
Nov 10, 2021	2.0.0	ADD - 1.2.4 Ensure Red Hat Subscription Manager connection is configured
Nov 10, 2021	2.0.0	ADD - 1.2.5 Disable the rhnsd Daemon
Nov 10, 2021	2.0.0	MOVE - 1.2.7 Ensure removal of software components after update Moved from section "System Maintenance" to subsection "1.2 - Configure Software Updates"
Nov 10, 2021	2.0.0	UPDATE - 1.3.2 Ensure filesystem integrity is regularly checked Audit Procedure: Improve commands used to check cron and systemd timer Remediation Procedure: Added examples for creating systemd timers as an option
Nov 10, 2021	2.0.0	UPDATE - 1.3.4 Ensure AIDE is configured to verify XATTRS Assessment Status: Changed to Manual. Automated Assessment Content (AAC) was unreliable
Nov 10, 2021	2.0.0	UPDATE - 1.3.5 Ensure AIDE is configured to use FIPS 140-2 Assessment Status: Changed to Manual. AAC was unreliable
Nov 10, 2021	2.0.0	UPDATE - 1.4.1 Ensure bootloader password is set Audit Procedure: Changed to script to account for either bios or UEFI boot Remediation Procedure: Updated to account for either bios or UEFI boot
Nov 10, 2021	2.0.0	UPDATE - 1.4.2 Ensure permissions on bootloader config are configured Audit Procedure: Changed to script to account for either bios or UEFI boot Remediation Procedure: Updated to account for either bios or UEFI boot
Nov 10, 2021	2.0.0	DELETE - Ensure UEFI requires authentication for single-user and maintenance modes
Nov 10, 2021	2.0.0	ADD - 1.4.5 Ensure version 7.2 or newer booted with a BIOS have a unique name for the grub superusers account
Nov 10, 2021	2.0.0	ADD - 1.4.6 Ensure version 7.2 or newer booted with UEFI have a unique name for the grub superusers account
Nov 10, 2021	2.0.0	UPDATE - 1.6.1.1 Ensure SELinux is installed Profile: Moved to Level 1 Server and Workstation

Nov 10, 2021	2.0.0	UPDATE - 1.6.1.2 Ensure SELinux is not disabled in bootloader configuration Profile: moved to level 1 server and workstation Audit Procedure: Updated command to account for either bios or UEFI boot Remediation Procedure: Updated to account for either bios or UEFI boot
Nov 10, 2021	2.0.0	UPDATE - 1.6.1.3 Ensure SELinux policy is configured Applicable Profiles: moved to Level 1 server and workstation
Nov 10, 2021	2.0.0	ADD - 1.6.1.4 Ensure the SELinux mode is enforcing or permissive
Nov 10, 2021	2.0.0	DELETE - Ensure the SELinux state is enforcing
Nov 10, 2021	2.0.0	ADD - 1.6.1.5 Ensure the SELinux mode is enforcing
Nov 10, 2021	2.0.0	DELETE - Ensure no unconfined daemons exist
Nov 10, 2021	2.0.0	ADD - 1.6.1.6 Ensure no unconfined services exist
Nov 10, 2021	2.0.0	ADD - 1.6.1.9 Ensure non-privileged users are prevented from executing privileged functions
Nov 10, 2021	2.0.0	MOVE - 1.6.1.10 Ensure system device files are labeled Moved from section "System Maintenance" to subsection "1.6.1 - Configure SELinux"
Nov 10, 2021	2.0.0	MOVE – Subsection - Command Line Warning Banners Moved from subsection "Warning Banners" to section "Initial Setup"
Nov 10, 2021	2.0.0	MOVE - 1.8.2 Ensure GDM login banner is configured Moved from subsection "Warning Banners" to subsection "1.8 GNOME Display Manager"
NOV 10, 2021	2.0.0	DELETE – Warning Banners
Nov 10, 2021	2.0.0	ADD – 1.8 GNOME Display Manager
Nov 10, 2021	2.0.0	ADD - 1.8.1 Ensure GNOME Display Manager is removed
Nov 10, 2021	2.0.0	UPDATE - 1.8.2 Ensure GDM login banner is configured Audit Procedure: change audit procedure Remediation Procedure: change remediation procedure
Nov 10, 2021	2.0.0	ADD - 1.8.3 Ensure last logged in user display is disabled
Nov 10, 2021	2.0.0	ADD - 1.8.4 Ensure XDCMP is not enabled
Nov 10, 2021	2.0.0	ADD - 1.8.5 Ensure Standard Mandatory DoD Notice and Consent Banner displayed via a graphical user logon
Nov 10, 2021	2.0.0	MOVE - 1.8.6 Ensure GDM session lock is enabled moved from subsection "GNOME Configuration" to subsection "1.8 - GNOME Display Manager"

Nov 10, 2021	2.0.0	ADD - 1.8.7 Ensure the graphical user Ctrl-Alt-Delete key sequence is disabled
Nov 10, 2021	2.0.0	ADD - 1.8.8 Ensure users must authenticate users using MFA via a graphical user logon
Nov 10, 2021	2.0.0	MOVE - 1.8.9 Ensure GNOME Screensaver period of inactivity is configured moved from subsection "GNOME Configuration" to subsection "1.8 - GNOME Display Manager"
Nov 10, 2021	2.0.0	MOVE - 1.8.10 Ensure screensaver lock-enabled is set moved from subsection "GNOME Configuration" to subsection "1.8 - GNOME Display Manager"
Nov 10, 2021	2.0.0	MOVE - 1.8.11 Ensure overriding the screensaver lock-delay setting is prevented moved from subsection "GNOME Configuration" to subsection "1.8 - GNOME Display Manager"
Nov 10, 2021	2.0.0	MOVE - 1.8.12 Ensure session idle-delay settings is enforced moved from subsection "GNOME Configuration" to subsection "1.8 - GNOME Display Manager"
Nov 10, 2021	2.0.0	MOVE - 1.8.13 Ensure GNOME Idle activation is set moved from subsection "GNOME Configuration" to subsection "1.8 - GNOME Display Manager"
Nov 10, 2021	2.0.0	MOVE - 1.8.14 Ensure the screensaver idle-activation-enabled setting moved from subsection "GNOME Configuration" to subsection "1.8 - GNOME Display Manager"
NOV 10, 2021	2.0.0	MOVE - 1.8.15 Ensure GNOME Lock Delay is configured - moved from subsection "GNOME Configuration" to subsection "1.8 - GNOME Display Manager"
Nov 10, 2021	2.0.0	MOVE - 1.8.16 Ensure automatic logon via GUI is not allowed moved from subsection "GNOME Configuration" to subsection "1.8 - GNOME Display Manager"
Nov 10, 2021	2.0.0	ADD - 1.8.17 Ensure unrestricted logon is not allowed
Nov 10, 2021	2.0.0	ADD - 1.8.18 Ensure graphical user interface automounter is disabled
Nov 10, 2021	2.0.0	ADD - 2.1.1 Ensure xinetd is not installed
Nov 10, 2021	2.0.0	DELETE - Ensure chargen services are not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure daytime services are not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure discard services are not enabled
Nov 10, 2020	2.0.0	DELETE - Ensure echo services are not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure time services are not enabled

Nov 10, 2021	2.0.0	DELETE - Ensure rsh server is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure talk server is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure telnet server is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure tftp server is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure xinetd is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure the ypserv package has been removed
Nov 10, 2021	2.0.0	UPDATE - 2.2.1.2 Ensure chrony is configured Audit Procedure: update commands used for audit Remediation Procedure: Add additional remediation step
Nov 10, 2021	2.0.0	UPDATE - 2.2.1.3 Ensure ntp is configured Audit Procedure: update commands used for audit Remediation Procedure: update remediation to work with systemd
Nov 10, 2021	2.0.0	DELETE - Ensure NTP "maxpoll" is set
Nov 10, 2021	2.0.0	ADD - 2.2.1.4 Ensure internal information system clocks are synchronizing
Nov 10, 2021	2.0.0	DELETE - GNOME Configuration - subsection deleted
Nov 10, 2021	2.0.0	DELETE - Ensure X Window System is not installed
Nov 10, 2021	2.0.0	DELETE - Ensure Avahi Server is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure CUPS is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure DHCP Server is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure LDAP server is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure NFS and RPC are not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure DNS Server is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure FTP Server is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure HTTP server is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure IMAP and POP3 server is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure Samba is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure HTTP Proxy Server is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure SNMP Server is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure rsync service is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure NIS Server is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure rsync service is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure NIS Server is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure NFS is configured to use RPCSEC_GSS
Nov 10, 2021	2.0.0	DELETE - Ensure noexec option is configured for NFS
Nov 10, 2021	2.0.0	ADD - 2.2.2 Ensure X11 Server components are not installed
Nov 10, 2021	2.0.0	ADD - 2.2.3 Ensure Avahi Server is not installed

Nov 10, 2021	2.0.0	ADD – 2.2.4 Ensure CUPS is not installed
Nov 10, 2021	2.0.0	ADD – 2.2.5 Ensure DHCP Server is not installed
Nov 10, 2021	2.0.0	ADD – 2.2.6 Ensure LDAP server is not installed
Nov 10, 2021	2.0.0	ADD – 2.2.7 Ensure DNS Server is not installed
Nov 10, 2021	2.0.0	ADD – 2.2.8 Ensure FTP Server is not installed
Nov 10, 2021	2.0.0	ADD – 2.2.9 Ensure HTTP server is not installed
Nov 10, 2021	2.0.0	ADD - 2.2.10 Ensure IMAP and POP3 server is not installed
Nov 10, 2021	2.0.0	ADD - 2.2.11 Ensure Samba is not installed
Nov 10, 2021	2.0.0	ADD - 2.2.12 Ensure HTTP Proxy Server is not installed
Nov 10, 2021	2.0.0	ADD - 2.2.13 Ensure net-snmp is not installed
Nov 10, 2021	2.0.0	ADD - 2.2.14 Ensure NIS server is not installed
Nov 10, 2021	2.0.0	ADD - 2.2.15 Ensure telnet-server is not installed
Nov 10, 2021	2.0.0	UPDATE - 2.2.16 Ensure mail transfer agent is configured for local-only mode Remediation Procedure: command updated for systemd command only
Nov 10, 2021	2.0.0	ADD - 2.2.17 Ensure nfs-utils is not installed or the nfs-server service is masked
Nov 10, 2021	2.0.0	ADD - 2.2.18 Ensure rpcbind is not installed or the rpcbind services are masked
Nov 10, 2021	2.0.0	ADD - 2.2.19 Ensure rsync is not installed or the rsyncd service is masked
Nov 10, 2021	2.0.0	ADD - 2.2.20 Ensure the rsh package has been removed
Nov 10, 2021	2.0.0	ADD - 2.2.21 Ensure the TFTP server has not been installed
Nov 10, 2021	2.0.0	ADD - 2.2.22 Ensure TFTP daemon is configured to operate in secure mode
Nov 10, 2021	2.0.0	UPDATE - 2.3.1 Ensure NIS Client is not installed Remediation Procedure: verbiage updated for clarification
Nov 10, 2021	2.0.0	UPDATE - 2.3.2 Ensure rsh client is not installed Remediation Procedure: verbiage updated for clarification
Nov 10, 2021	2.0.0	UPDATE - 2.3.3 Ensure talk client is not installed Remediation Procedure: verbiage updated for clarification
Nov 10, 2021	2.0.0	UPDATE - 2.3.4 Ensure telnet client is not installed Remediation Procedure: verbiage updated for clarification
Nov 10, 2021	2.0.0	UPDATE - 2.3.5 Ensure LDAP client is not installed Remediation Procedure: verbiage updated for clarification
Nov 10, 2021	2.0.0	ADD - 2.4 Ensure nonessential services are removed or masked

Nov 10, 2021	2.0.0	ADD - 3.1 Disable unused network protocols and devices – Subsection added
Nov 10, 2021	2.0.0	MOVE - 3.1.1 Disable IPv6 Moved from section “Network Configuration” into subsection “3.1 Disable unused network protocols and devices”
Nov 10, 2021	2.0.0	UPDATE - 3.1.1 Disable IPv6 Impact Statement: added Audit Procedure: added option for disabling IPv6 through systemctl configuration files Remediation Procedure: added option for disabling IPv6 through systemctl configuration files
Nov 10, 2021	2.0.0	MOVE - 3.1.2 Ensure wireless interfaces are disabled moved for section “Network Configuration” into subsection “3.1 Disable unused network protocols and devices”
Nov 10, 2021	2.0.0	UPDATE - 3.2 Network Parameters (Host Only) Overview: add Note about systemctl settings
Nov 10, 2021	2.0.0	UPDATE - 3.2.1 Ensure IP forwarding is disabled Audit Procedure: add coverage for IPv6, update command to include additional config directories Remediation Procedure: add coverage for IPv6
Nov 10, 2021	2.0.0	UPDATE – 3.2.2 Ensure packet redirect sending is disabled Audit Procedure: update command to include additional config directories
Nov 10, 2021	2.0.0	UPDATE - 3.3.1 Ensure source routed packets are not accepted Audit Procedure: add coverage for IPv6, update command to include additional config directories Remediation Procedure: add coverage for IPv6
Nov 10, 2021	2.0.0	UPDATE - 3.3.2 Ensure ICMP redirects are not accepted Audit Procedure: add coverage for IPv6, update command to include additional config directories Remediation Procedure: add coverage for IPv6
Nov 10, 2021	2.0.0	UPDATE - 3.3.4 Ensure secure ICMP redirects are not accepted Audit Procedure: update command to include additional config directories
Nov 10, 2021	2.0.0	UPDATE - 3.3.5 Ensure suspicious packets are logged Audit Procedure: update command to include additional config directories

Nov 10, 2021	2.0.0	UPDATE - 3.3.6 Ensure broadcast ICMP requests are ignored Audit Procedure: update command to include additional config directories
Nov 10, 2021	2.0.0	UPDATE - 3.3.7 Ensure bogus ICMP responses are ignored Audit Procedure: update command to include additional config directories
Nov 10, 2021	2.0.0	UPDATE - 3.3.8 Ensure Reverse Path Filtering is enabled Audit Procedure: update command to include additional config directories
Nov 10, 2021	2.0.0	UPDATE - 3.3.9 Ensure TCP SYN Cookies is enabled Audit Procedure: update command to include additional config directories
Nov 10, 2021	2.0.0	DELETE - Ensure rate limiting measures are set
Nov 10, 2021	2.0.0	ADD - 3.3.10 Ensure IPv6 router advertisements are not accepted
Nov 10, 2021	2.0.0	DELETE - TCP Wrappers
Nov 10, 2021	2.0.0	DELETE - Ensure TCP Wrappers is installed
Nov 10, 2021	2.0.0	DELETE - Ensure /etc/hosts.allow is configured
Nov 10, 2021	2.0.0	DELETE - Ensure /etc/hosts.deny is configured
Nov 10, 2021	2.0.0	DELETE - Ensure permissions on /etc/hosts.allow are configured
Nov 10, 2021	2.0.0	DELETE - Ensure permissions on /etc/hosts.deny are configured
Nov 10, 2021	2.0.0	DELETE - Ensure RDS is disabled
Nov 10, 2021	2.0.0	DELETE - Ensure TIPC is disabled
Nov 10, 2021	2.0.0	UPDATE - 3.5.1 Configure firewalld Overview: Added statement for clarification. Added Note
Nov 10, 2021	2.0.0	DELETE - Ensure Firewall software is installed
Nov 10, 2021	2.0.0	DELETE - Ensure a Firewall package is installed
Nov 10, 2021	2.0.0	DELETE - Ensure iptables is not running and masked
Nov 10, 2021	2.0.0	DELETE - Ensure nftables is not enabled
Nov 10, 2021	2.0.0	DELETE - Ensure default zone is set
Nov 10, 2021	2.0.0	DELETE - Ensure default zone is set to public
Nov 10, 2021	2.0.0	DELETE - Ensure unnecessary services and ports are not accepted
Nov 10, 2021	2.0.0	ADD - 3.5.1.1 - Ensure firewalld is installed
Nov 10, 2021	2.0.0	ADD - 3.5.1.2 Ensure iptables-services not installed with firewalld
Nov 10, 2021	2.0.0	ADD - 3.5.1.3 Ensure nftables either not installed or masked with firewalld
Nov 10, 2021	2.0.0	UPDATE - 3.5.1.4 Ensure firewalld service enabled and running Remediation Procedure: add command to unmask firewalld service
Nov 10, 2021	2.0.0	ADD - 3.5.1.5 Ensure firewalld default zone is set

Nov 10, 2021	2.0.0	UPDATE - 3.5.1.6 Ensure network interfaces are assigned to appropriate zone Audit Procedure: change command to work without the nmcli command Additional Information: re-written to clarify and add example
Nov 10, 2021	2.0.0	ADD - 3.5.1.7 Ensure firewalld drops unnecessary services and ports
Nov 10, 2021	2.0.0	UPDATE - 3.5.2 Configure nftables Overview: added statement for clarification. Added Note
Nov 10, 2021	2.0.0	DELETE - Ensure iptables are flushed
Nov 10, 2021	2.0.0	DELETE - Ensure default deny firewall policy
Nov 10, 2021	2.0.0	DELETE - Ensure a table exists
Nov 10, 2021	2.0.0	DELETE - Ensure base chains exist
Nov 10, 2021	2.0.0	DELETE - Ensure loopback traffic is configured
Nov 10, 2021	2.0.0	DELETE - Ensure outbound and established connections are configured
Nov 10, 2021	2.0.0	ADD - 3.5.2.1 - Ensure nftables is installed
Nov 10, 2021	2.0.0	ADD - 3.5.2.2 Ensure firewalld is either not installed or masked with nftables
Nov 10, 2021	2.0.0	ADD - 3.5.2.3 Ensure iptables-services not installed with nftables
Nov 10, 2021	2.0.0	ADD - 3.5.2.4 Ensure iptables are flushed with nftables
Nov 10, 2021	2.0.0	ADD - 3.5.2.5 Ensure an nftables table exists
Nov 10, 2021	2.0.0	ADD - 3.5.2.6 Ensure nftables base chains exist
Nov 10, 2021	2.0.0	ADD - 3.5.2.7 Ensure nftables loopback traffic is configured
Nov 10, 2021	2.0.0	ADD - 3.5.2.7 Ensure nftables loopback traffic is configured
Nov 10, 2021	2.0.0	ADD - 3.5.2.9 Ensure nftables default deny firewall policy
Nov 10, 2021	2.0.0	UPDATE - 3.5.3 Configure iptables Overview: added statement for clarification. Added Note
Nov 10, 2021	2.0.0	DELETE - Ensure iptables is installed
Nov 10, 2021	2.0.0	ADD - 3.5.3.1 Configure iptables software
Nov 10, 2021	2.0.0	ADD - 3.5.3.1.1 Ensure iptables packages are installed
Nov 10, 2021	2.0.0	ADD - 3.5.3.1.2 Ensure nftables is not installed with iptables
Nov 10, 2021	2.0.0	ADD - 3.5.3.1.3 Ensure firewalld is either not installed or masked with iptables
Nov 10, 2021	2.0.0	UPDATE - 3.5.3.2 Configure IPv4 iptables Overview: reformatted for clarification, added statement about openSSH port
Nov 10, 2021	2.0.0	DELETE - Ensure default deny firewall policy
Nov 10, 2021	2.0.0	DELETE - Ensure loopback traffic is configured

Nov 10, 2021	2.0.0	DELETE - Ensure outbound and established connections are configured
Nov 10, 2021	2.0.0	DELETE - Ensure firewall rules exist for all open ports
Nov 10, 2021	2.0.0	ADD - 3.5.3.2.1 Ensure iptables loopback traffic is configured
Nov 10, 2021	2.0.0	ADD - 3.5.3.2.2 Ensure iptables outbound and established connections are configured
Nov 10, 2021	2.0.0	ADD - 3.5.3.2.3 Ensure iptables rules exist for all open ports
Nov 10, 2021	2.0.0	ADD - 3.5.3.2.4 Ensure iptables default deny firewall policy
Nov 10, 2021	2.0.0	ADD - 3.5.3.2.5 Ensure iptables rules are saved
Nov 10, 2021	2.0.0	ADD - 3.5.3.2.6 Ensure iptables is enabled and running
Nov 10, 2021	2.0.0	UPDATE - 3.5.3.3 Configure IPv6 ip6tables Overview: reformatted for clarification, added statement about openSSH port
Nov 10, 2021	2.0.0	DELETE - Ensure IPv6 default deny firewall policy
Nov 10, 2021	2.0.0	DELETE - Ensure IPv6 loopback traffic is configured
Nov 10, 2021	2.0.0	DELETE - Ensure IPv6 outbound and established connections are configured
Nov 10, 2021	2.0.0	DELETE - Ensure IPv6 firewall rules exist for all open ports
Nov 10, 2021	2.0.0	ADD - 3.5.3.3.1 Ensure ip6tables loopback traffic is configured
Nov 10, 2021	2.0.0	ADD - 3.5.3.3.2 Ensure ip6tables outbound and established connections are configured
Nov 10, 2021	2.0.0	ADD - 3.5.3.3.3 Ensure ip6tables firewall rules exist for all open ports
Nov 10, 2021	2.0.0	ADD - 3.5.3.3.4 Ensure ip6tables default deny firewall policy
Nov 10, 2021	2.0.0	ADD - 3.5.3.3.5 Ensure ip6tables rules are saved
Nov 10, 2021	2.0.0	ADD - 3.5.3.3.6 Ensure ip6tables is enabled and running
Nov 10, 2021	2.0.0	DELETE - Ensure iptables is installed
Nov 10, 2021	2.0.0	UPDATE - 4.1 Configure System Accounting (auditd) Overview: Added additional bullets to Note
Nov 10, 2021	2.0.0	DELETE - Ensure auditd service is enabled
Nov 10, 2021	2.0.0	ADD - 4.1.1.1 Ensure auditd is installed
Nov 10, 2021	2.0.0	MOVE - 4.1.1.1 Ensure auditd is installed Moved into subsection "4.1.1.1 Ensure auditd is installed"
Nov 10, 2021	2.0.0	ADD - 4.1.1.2 Ensure auditd service is enabled and running
Nov 10, 2021	2.0.0	MOVE - 4.1.1.3 Ensure auditing for processes that start prior to auditd is enabled Moved into subsection "4.1.1.1 Ensure auditd is installed"

Nov 10, 2021	2.0.0	UPDATE - 4.1.1.3 Ensure auditing for processes that start prior to auditd is enabled Audit Procedure: added support for UEFI boot Remediation Procedure: added support for UEFI boot
Nov 10, 2021	2.0.0	UPDATE - 4.1.2.1 Ensure audit log storage size is configured Description: Added notes
Nov 10, 2021	2.0.0	MOVE - 4.1.2.3 Ensure audit system is set to single when the disk is full Moved into subsection "4.1.2 - Configure Data Retention"
Nov 10, 2021	2.0.0	MOVE - 4.1.2.4 Ensure system notification is sent out when volume is 75% full Moved into subsection "4.1.2 - Configure Data Retention"
Nov 10, 2021	2.0.0	MOVE - 4.1.2.6 Ensure audit system action is defined for sending errors Moved into subsection "4.1.2 - Configure Data Retention"
Nov 10, 2021	2.0.0	ADD - 4.1.2.7 Ensure audit_backlog_limit is sufficient
Nov 10, 2021	2.0.0	MOVE - 4.1.2.10 Ensure the auditing processing failures are handled Moved to subsection "4.1.2 - Configure Data Retention"
Nov 10, 2021	2.0.0	MOVE - 4.1.2.11 Ensure off-load of audit logs Moved into subsection "4.1.2 - Configure Data Retention"
Nov 10, 2021	2.0.0	MOVE - 4.1.2.12 Ensure action is taken when audisp-remote buffer is full Moved into subsection "4.1.2 - Configure Data Retention"
Nov 10, 2021	2.0.0	MOVE - 4.1.2.13 Ensure off-loaded audit logs are labeled Moved into subsection "4.1.2 - Configure Data Retention"
Nov 10, 2021	2.0.0	DELETE - Configure audit of commands
Nov 10, 2021	2.0.0	ADD - 4.1.3 - Configure auditd rules
Nov 10, 2021	2.0.0	UPDATE - 4.1.3.1 Ensure events that modify date and time information are collected Moved into subsection "4.1.3 - Configure auditd rules" Remediation Procedure: updated example
Nov 10, 2021	2.0.0	DELETE - Ensure system administrator actions (sudolog) are collected
Nov 10, 2021	2.0.0	ADD - 4.1.3.2 Ensure system administrator command executions (sudo) are collected
Nov 10, 2021	2.0.0	UPDATE - 4.1.3.3 Ensure session initiation information is collected Moved into subsection "4.1.3 - Configure auditd rules" Remediation Procedure: updated example

Nov 10, 2021	2.0.0	UPDATE - 4.1.3.4 Ensure events that modify the system's Mandatory Access Controls are collected Moved into subsection "4.1.3 - Configure auditd rules" Description: removed references to AppArmor, added notes Remediation Procedure: updated example
Nov 10, 2021	2.0.0	UPDATE - 4.1.3.5 Ensure events that modify the system's network environment are collected Moved into subsection "4.1.3 - Configure auditd rules" Remediation Procedure: updated example
Nov 10, 2021	2.0.0	UPDATE - 4.1.3.6 Ensure successful file system mounts are collected Moved into subsection "4.1.3 - Configure auditd rules" Remediation Procedure: updated example
Nov 10, 2021	2.0.0	UPDATE - 4.1.3.7 Ensure kernel module loading and unloading is collected Moved into subsection "4.1.3 - Configure auditd rules" Remediation Procedure: updated example
Nov 10, 2021	2.0.0	UPDATE - 4.1.3.8 Ensure changes to system administration scope (sudoers) is collected Moved into subsection "4.1.3 - Configure auditd rules" Remediation Procedure: updated example
Nov 10, 2021	2.0.0	UPDATE - 4.1.3.9 Ensure file deletion events by users are collected Moved into subsection "4.1.3 - Configure auditd rules" Remediation Procedure: updated example
Nov 10, 2021	2.0.0	UPDATE - 4.1.3.10 Ensure use of privileged commands is collected Moved into subsection "4.1.3 - Configure auditd rules" Remediation Procedure: updated example
Nov 10, 2021	2.0.0	UPDATE - 4.1.3.11 Ensure unsuccessful unauthorized file access attempts are collected Moved into subsection "4.1.3 - Configure auditd rules" Description: added note Remediation Procedure: updated example
Nov 10, 2021	2.0.0	UPDATE - 4.1.3.12 Ensure discretionary access control permission modification events are collected Moved into subsection "4.1.3 - Configure auditd rules" Description: added note Remediation Procedure: updated example

Nov 10, 2021	2.0.0	UPDATE - 4.1.3.13 Ensure login and logout events are collected Moved into subsection "4.1.3 - Configure auditd rules" Description: added note Remediation Procedure: updated example
Nov 10, 2021	2.0.0	UPDATE - 4.1.3.14 Ensure events that modify user/group information are collected Moved into subsection "4.1.3 - Configure auditd rules" Description: added note Remediation Procedure: updated example
Nov 10, 2021	2.0.0	MOVE - 4.1.3.15 Ensure all uses of the passwd command are audited Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.16 Ensure auditing of the unix_chkpwd command Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.17 Ensure audit of the gpasswd command Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.18 Ensure audit all uses of chage Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.19 Ensure audit all uses of the chsh command Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.20 Ensure audit the umount command Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.21 Ensure audit of postdrop command Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.22 Ensure audit of postqueue command Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.23 Ensure audit ssh-keygen command Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.24 Ensure audit of crontab command Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.25 Ensure audit of kmod command Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.26 Ensure audit of the rmdir syscall Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.27 Ensure audit of unlink syscall Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.28 Ensure audit unlinkat syscall Moved into subsection "4.1.3 - Configure auditd rules"

Nov 10, 2021	2.0.0	MOVE - 4.1.3.29 Ensure audit pam_timestamp_check command Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.30 Ensure audit of the finit_module syscall Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.31 Ensure audit of the create_module syscall Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.32 Ensure auditing of all privileged functions Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.33 Ensure audit of semanage command Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.34 Ensure audit of the setsebool command Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.35 Ensure audit of the chcon command Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.36 Ensure audit of the userhelper command Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.37 Ensure audit of the mount command and syscall Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.38 Ensure audit of the su command Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.39 Ensure audit of setfiles command Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.40 Ensure audit all uses of the newgrp command Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	MOVE - 4.1.3.41 Ensure the audit configuration is immutable Moved into subsection "4.1.3 - Configure auditd rules"
Nov 10, 2021	2.0.0	ADD - 4.1.4 Configure auditd file access
Nov 10, 2021	2.0.0	ADD - 4.1.4.1 Ensure Audit logs are owned by root and mode 0600 or less permissive
Nov 10, 2021	2.0.0	DELETE - Ensure rsyslog Service is enabled
Nov 10, 2021	2.0.0	ADD - 4.2.1.2 Ensure rsyslog Service is enabled and running
Nov 10, 2021	2.0.0	UPDATE - 4.2.1.3 Ensure rsyslog default file permissions configured Description: added notes Additional Information: Moved to Notes in Description

Nov 10, 2021	2.0.0	UPDATE - 4.2.1.5 Ensure rsyslog is configured to send logs to a remote log host Description: Added note Audit Procedure: Added command to accept newer syntax Remediation Procedure: Added option for newer syntax
Nov 10, 2021	2.0.0	UPDATE - 4.2.1.6 Ensure remote rsyslog messages are only accepted on designated log hosts. Description: Added note
Nov 10, 2021	2.0.0	DELETE - Ensure rsyslog imudp and imrelp aren't loaded
Nov 10, 2021	2.0.0	DELETE - Configure cron
Nov 10, 2021	2.0.0	ADD - 5.1 Configure time-based job schedulers
Nov 10, 2021	2.0.0	UPDATE - 5.1.1 Ensure cron daemon is enabled and running Moved from subsection "Configure cron" to subsection "5. 1 Configure time-based job schedulers Audit Procedure: removed chkconfig command, added systemctl status check Remediation Procedure: removed chkconfig command, removed update-rc.d, added option to uninstall cronie if systemd times are used instead of cron
Nov 10, 2021	2.0.0	MOVE - 5.1.2 Ensure permissions on /etc/crontab are configured Moved from subsection "Configure cron" to subsection "5. 1 Configure time-based job schedulers
Nov 10, 2021	2.0.0	MOVE - 5.1.3 Ensure permissions on /etc/cron.hourly are configured Moved from subsection "Configure cron" to subsection "5. 1 Configure time-based job schedulers
Nov 10, 2021	2.0.0	MOVE - 5.1.4 Ensure permissions on /etc/cron.daily are configured Moved from subsection "Configure cron" to subsection "5. 1 Configure time-based job schedulers
Nov 10, 2021	2.0.0	MOVE - 5.1.5 Ensure permissions on /etc/cron.weekly are configured Moved from subsection "Configure cron" to subsection "5. 1 Configure time-based job schedulers
Nov 10, 2021	2.0.0	MOVE - 5.1.6 Ensure permissions on /etc/cron.monthly are configured Moved from subsection "Configure cron" to subsection "5. 1 Configure time-based job schedulers
Nov 10, 2021	2.0.0	MOVE - 5.1.7 Ensure permissions on /etc/cron.d are configured Moved from subsection "Configure cron" to subsection "5. 1 Configure time-based job schedulers
Nov 10, 2021	2.0.0	DELETE - Ensure at/cron is restricted to authorized users

Nov 10, 2021	2.0.0	ADD - 5.1.8 Ensure cron is restricted to authorized users
Nov 10, 2021	2.0.0	ADD - 5.1.9 Ensure at is restricted to authorized users
Nov 10, 2021	2.0.0	MOVE - 5.2 Configure sudo Moved from section: "1 - Initial Setup" to section: "5 - Access, Authentication and Authorization"
Nov 10, 2021	2.0.0	UPDATE - 5.2.1 Ensure sudo is installed Remediation Procedure: corrected command (dnf changed to yum)
Nov 10, 2021	2.0.0	UPDATE - 5.2.2 Ensure sudo commands use pty Description: Add note about visudo Rationale Statement: added additional information Audit Procedure: updated audit command to fix error
Nov 10, 2021	2.0.0	UPDATE - 5.2.2 Ensure sudo commands use pty Description: Add note about visudo Audit Procedure: updated audit command Remediation Procedure: Updated text for clarification
Nov 10, 2021	2.0.0	MOVE - 5.2.4 Ensure users must provide password for escalation Moved from subsection: "User Accounts and Environment" to subsection: "5.2 - Configure sudo"
Nov 10, 2021	2.0.0	MOVE - 5.2.5 Ensure users must re-authenticate for privilege escalation Moved from subsection: "User Accounts and Environment" to subsection: "5.2 - Configure sudo"
Nov 10, 2021	2.0.0	ADD - 5.2.6 Ensure the sudoers file restricts sudo access to authorized personnel
Nov 10, 2021	2.0.0	ADD - 5.2.7 Ensure sudo authentication timeout is configured
Nov 10, 2021	2.0.0	ADD - 5.2.8 Ensure users password required for privilege escalation when using sudo
Nov 10, 2021	2.0.0	UPDATE - 5.3 Configure SSH Server Title: changed from: "SSH Server Configuration" to: "Configure SSH Server" Overview: added additional information
Nov 10, 2021	2.0.0	DELETE - Ensure SSH MaxSessions is set to 4 or less
Nov 10, 2021	2.0.0	DELETE - Ensure only FIPS 140-2 MACs are used for SSH
Nov 10, 2021	2.0.0	DELETE - Ensure remote X connections are encrypted.
Nov 10, 2021	2.0.0	UPDATE - 5.3.4 Ensure permissions on SSH private host key files are configured Audit Procedure: updated to allow either group root or ssh_keys Remediation Procedure: updated to allow either group root or ssh_keys

Nov 10, 2021	2.0.0	UPDATE - 5.3.6 Ensure SSH access is limited Audit Procedure: Updated audit commands
Nov 10, 2021	2.0.0	UPDATE - 5.3.7 Ensure SSH LogLevel is appropriate Audit Procedure: Updated audit commands
Nov 10, 2021	2.0.0	UPDATE - 5.3.8 Ensure SSH X11 forwarding is disabled Audit Procedure: Updated audit commands
Nov 10, 2021	2.0.0	UPDATE - 5.3.9 Ensure SSH MaxAuthTries is set to 4 or less Audit Procedure: Updated audit commands
Nov 10, 2021	2.0.0	UPDATE - 5.3.10 Ensure SSH IgnoreRhosts is enabled Audit Procedure: Updated audit commands
Nov 10, 2021	2.0.0	UPDATE - 5.3.11 Ensure SSH HostbasedAuthentication is disabled Audit Procedure: Updated audit commands
Nov 10, 2021	2.0.0	UPDATE - 5.3.12 Ensure SSH root login is disabled Audit Procedure: Updated audit commands
Nov 10, 2021	2.0.0	UPDATE - 5.3.13 Ensure SSH PermitEmptyPasswords is disabled Audit Procedure: Updated audit commands
Nov 10, 2021	2.0.0	UPDATE - 5.3.14 Ensure SSH PermitUserEnvironment is disabled Audit Procedure: Updated audit commands
Nov 10, 2021	2.0.0	UPDATE - 5.3.15 Ensure only strong Ciphers are used Audit Procedure: Updated audit commands. Moved “Weak Ciphers” list to additional information section
Nov 10, 2021	2.0.0	UPDATE - 5.3.17 Ensure only strong MAC algorithms are used Audit Procedure: Updated audit commands. Moved “Weak MAC algorithms” list to additional information section
Nov 10, 2021	2.0.0	UPDATE - 5.3.18 Ensure only strong Key Exchange algorithms are used Audit Procedure: Updated audit commands. Moved “Weak Key Exchange Algorithms” list to additional information section
Nov 10, 2021	2.0.0	UPDATE - 5.3.19 Ensure SSH Idle Timeout Interval is configured Audit Procedure: Updated audit commands and expected values Remediation Procedure: Updated values
Nov 10, 2021	2.0.0	UPDATE - 5.3.20 Ensure SSH LoginGraceTime is set to one minute or less Audit Procedure: Updated audit commands
Nov 10, 2021	2.0.0	UPDATE - 5.3.21 Ensure SSH warning banner is configured Audit Procedure: Updated audit commands
Nov 10, 2021	2.0.0	UPDATE - 5.3.22 Ensure SSH PAM is enabled Audit Procedure: Updated audit commands

Nov 10, 2021	2.0.0	UPDATE - 5.3.23 Ensure SSH AllowTcpForwarding is disabled Audit Procedure: Updated audit commands
Nov 10, 2021	2.0.0	UPDATE - 5.3.24 Ensure SSH MaxStartups is configured Audit Procedure: Updated audit commands
Nov 10, 2021	2.0.0	ADD - 5.3.25 Ensure SSH MaxSessions is limited
Nov 10, 2021	2.0.0	UPDATE - 5.3.29 Ensure SSH Protocol is set to 2 Audit Procedure: Add note about release level applicability. Update audit command
Nov 10, 2021	2.0.0	ADD - 5.3.35 Ensure SSH X11UseLocalhost is enabled
Nov 10, 2021	2.0.0	UPDATE - 5.4.1 Ensure password creation requirements are configured Description: add information about minclass Audit Procedure: Include option to use minclass, update audit commands Remediation Procedure: Include option to use minclass
Nov 10, 2021	2.0.0	UPDATE - 5.4.2 Ensure lockout for failed password attempts is configured Description: add additional notes Audit Procedure: Updated to clarify Remediation Procedure: Updated to clarify
Nov 10, 2021	2.0.0	UPDATE - 5.4.3 Ensure password hashing algorithm is SHA-512 Description: add additional notes Audit Procedure: Updated to clarify Remediation Procedure: Updated to clarify
Nov 10, 2021	2.0.0	UPDATE - 5.4.4 Ensure password reuse is limited512 Description: add additional notes Audit Procedure: Updated to clarify Remediation Procedure: Updated to clarify
Nov 10, 2021	2.0.0	ADD - 5.4.12 Ensure accounts lock for a minimum of 15 minutes after three unsuccessful logon attempts within a 15-minute timeframe
Nov 10, 2021	2.0.0	ADD - 5.4.13 Ensure lockout for unsuccessful root logon attempts
Nov 10, 2021	2.0.0	UPDATE - 5.5.1.2 Ensure minimum days between password changes is configured Audit Procedure: Audit commands updated
Nov 10, 2021	2.0.0	UPDATE - 5.5.1.3 Ensure password expiration warning days is 7 or more Audit Procedure: Audit commands updated
Nov 10, 2021		ADD - 5.5.1.6 Ensure shadow file is configured to use only encrypted representations of passwords

Nov 10, 2021	2.0.0	DELETE - Ensure encrypted representation of passwords is set
Nov 10, 2021	2.0.0	DELETE - Ensure default user shell timeout is 600 seconds or less
Nov 10, 2021	2.0.0	ADD - 5.5.4 Ensure default user shell timeout is configured
Nov 10, 2021	2.0.0	DELETE - Ensure default user umask is 027 or more restrictive
Nov 10, 2021	2.0.0	ADD - 5.5.5 Ensure default user umask is configured
Nov 10, 2021	2.0.0	DELETE - Ensure default user umask is 077
Nov 10, 2021	2.0.0	ADD - 5.5.9 Ensure local interactive user accounts umask is 077
Nov 10, 2021	2.0.0	MOVE - 5.5.10 Ensure upon user creation a home directory is assigned Moved from subsection "User and Group Settings" to subsection "5.5 - User Accounts and Environment"
Nov 10, 2021	2.0.0	UPDATE - 5.7 Ensure access to the su command is restricted Audit Procedure: Updated audit commands Remediation Procedure: Updated procedure
Nov 10, 2021	2.0.0	UPDATE - 6.1.2 Ensure permissions on /etc/passwd are configured Remediation Procedure: Updated chmod to remove opposed to overwrite
Nov 10, 2021	2.0.0	UPDATE - 6.1.3 Ensure permissions on /etc/passwd- are configured Audit Procedure: Audit values changed to reflect permissions on /etc/passwd Remediation Procedure: Values updated
Nov 10, 2021	2.0.0	UPDATE - 6.1.4 Ensure permissions on /etc/shadow are configured Audit Procedure: Audit values changed Remediation Procedure: values changed
Nov 10, 2021	2.0.0	UPDATE - 6.1.5 Ensure permissions on /etc/shadow- are configured Audit Procedure: Audit values changed Remediation Procedure: values changed
Nov 10, 2021	2.0.0	UPDATE - 6.1.6 Ensure permissions on /etc/gshadow- are configured Audit Procedure: Audit values changed Remediation Procedure: values changed
Nov 10, 2021	2.0.0	UPDATE - 6.1.7 Ensure permissions on /etc/gshadow are configured Audit Procedure: Audit values changed Remediation Procedure: values changed
Nov 10, 2021	2.0.0	UPDATE - 6.1.8 Ensure permissions on /etc/group are configured Remediation Procedure: Updated chmod to remove opposed to overwrite
Nov 10, 2021	2.0.0	ADD - 6.1.15 Ensure the file permissions ownership and group membership of system files and commands match the vendor values

Nov 10, 2021	2.0.0	ADD - 6.1.16 Ensure all world-writable directories are owned by root, sys, bin, or an application User Identifier
Nov 10, 2021	2.0.0	DELETE - Ensure no legacy "+" entries exist in /etc/passwd
Nov 10, 2021	2.0.0	DELETE - Ensure no legacy "+" entries exist in /etc/shadow
Nov 10, 2021	2.0.0	DELETE - Ensure no legacy "+" entries exist in /etc/group
Nov 10, 2021	2.0.0	DELETE - Ensure password fields are not empty
Nov 10, 2021	2.0.0	ADD - 6.2.1 Ensure accounts in /etc/passwd use shadowed passwords
Nov 10, 2021	2.0.0	ADD - 6.2.2 Ensure /etc/shadow password fields are not empty
Nov 10, 2021	2.0.0	UPDATE - 6.2.4 Ensure shadow group is empty Audit Procedure: Audit commands updated Remediation Procedure: Commands added
Nov 10, 2021	2.0.0	UPDATE - 6.2.10 Ensure root PATH Integrity Audit Procedure: script updated for accuracy and clarification
Nov 10, 2021	2.0.0	UPDATE - 6.2.11 Ensure all users' home directories exist Audit Procedure: audit script simplified Remediation Procedure: Remediation script added
Nov 10, 2021	2.0.0	UPDATE - 6.2.12 Ensure users own their home directories Audit Procedure: audit script simplified Remediation Procedure: Remediation script added
Nov 10, 2021	2.0.0	UPDATE - 6.2.13 Ensure users' home directories permissions are 750 or more restrictive directories Audit Procedure: audit script simplified Remediation Procedure: Remediation script added
Nov 10, 2021	2.0.0	UPDATE - 6.2.14 Ensure users' dot files are not group or world writable Audit Procedure: audit script simplified Remediation Procedure: Remediation script added
Nov 10, 2021	2.0.0	UPDATE - 6.2.15 Ensure no users have .forward files Audit Procedure: audit script simplified Remediation Procedure: Remediation script added
Nov 10, 2021	2.0.0	UPDATE - 6.2.16 Ensure no users have .netrc files Rationale Statement: Updated to allow for restricted permissions where files are required Audit Procedure: Updated to allow for restricted permissions where files are required Remediation Procedure: Remediation script added
Nov 10, 2021	2.0.0	DELETE - Ensure users' .netrc Files are not group or world accessible

Nov 10, 2021	2.0.0	UPDATE - 6.2.17 Ensure no users have .rhosts files Audit Procedure: audit script simplified Remediation Procedure: Remediation script added
Nov 10, 2021	2.0.0	MOVE - 6.2.18 Ensure there are no unnecessary accounts Moved from subsection: "User Accounts and Environment" to subsection: "6.2 - User and Group Settings"