CIS Red Hat Enterprise Linux 9 STIG Benchmark

v1.0.0 - 04-29-2025

Terms of Use

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

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

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

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

Table of Contents

Overview

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

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

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

Important Usage Information

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

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

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

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

Key Stakeholders

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

Apply the Correct Version of a Benchmark

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

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.

- **Use the most recent version of a Benchmark**: This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

Exceptions

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

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

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

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

Remediation

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

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

The following is a reasonable remediation approach to follow:

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

Summary

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

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

CIS-CAT® Pro is also available to CIS SecureSuite® members.

Target Technology Details

Red Hat Enterprise Linux 9 Secure Technical Implementation Guide (STIG)
Version: 2 Release: 4 Benchmark
Date: 02 Apr 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Red Hat Enterprise Linux 9 and are looking to comply with the STIG guidance

Recommendation Definitions

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

Title

Concise description for the recommendation's intended configuration.

Assessment Status

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

Automated

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

Manual

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

Profile

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

Description

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

Rationale Statement

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

Impact Statement

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

Audit Procedure

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

Remediation Procedure

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

Default Value

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

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

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

Additional Information

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

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

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

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

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

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

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

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

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

  This profile is intended for servers and workstations.

Acknowledgements

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

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Red Hat Enterprise Linux 9

Editor
Eric Pinnell
Michael Wood
Randie Bejar
Gokhan Lus

Recommendations

1 STIG RULES

Red Hat Enterprise Linux 9

Secure Technical Implementation Guide (STIG)

Version: 2 Release: 4 Benchmark

Date: 02 Apr 2025

CLASSIFICATION unclassified

1.1 RHEL-09-171011 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must display the Standard Mandatory DOD Notice and Consent Banner before granting local or remote access to the system via a graphical user logon.

```
GROUP ID: V-270174
RULE ID: SV-270174r1044831
```

Rationale:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via logon interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with applicable DOD policy. Use the following verbiage for operating systems that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000228-GPOS-00088

Audit:

Note: This requirement assumes the use of the RHEL 9 default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.
Verify RHEL 9 displays the Standard Mandatory DOD Notice and Consent Banner before granting access to the operating system via a graphical user logon.
Check that the operating system displays the exact Standard Mandatory DOD Notice and Consent Banner text with the command:

```
$ gsettings get org.gnome.login-screen banner-message-text

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 interface.
If the banner does not match the Standard Mandatory DOD Notice and Consent Banner exactly, this is a finding.

Remediation:

Configure the operating system to display the Standard Mandatory DOD Notice and Consent Banner before granting access to the system.
Add the following lines to the [org/gnome/login-screen] section of the "/etc/dconf/db/local.d/01-banner-message":

```
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 interface.
Run the following command to update the database:

```
$ sudo dconf update
```

Additional Information:

CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53 :: AC-8 a
- NIST SP 800-53 Revision 4 :: AC-8 a
- NIST SP 800-53 Revision 5 :: AC-8 a
- NIST SP 800-53A :: AC-8.1 (ii)

1.2 RHEL-09-211010 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

RHEL 9 must be a vendor-supported release.

```
GROUP ID: V-257777
RULE ID: SV-257777r991589
```

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.

Audit:

Verify that the version or RHEL 9 is vendor supported with the following command:

```
$ cat /etc/redhat-release

Red Hat Enterprise Linux release 9.2 (Plow)
```

If the installed version of RHEL 9 is not supported, this is a finding.

Remediation:

Upgrade to a supported version of RHEL 9.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.3 RHEL-09-211015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 vendor packaged system security patches and updates must be installed and up to date.

```
GROUP ID: V-257778
RULE ID: SV-257778r991589
```

Rationale:

Installing software updates is a fundamental mitigation against the exploitation of publicly known vulnerabilities. If the most recent security patches and updates are not installed, unauthorized users may take advantage of weaknesses in the unpatched software. The lack of prompt attention to patching could result in a system compromise.

Audit:

Verify RHEL 9 security patches and updates are installed and up to date. Updates are required to be applied with a frequency determined by organizational policy.
Obtain the list of available package security updates from Red Hat. The URL for updates is https://access.redhat.com/errata-search/. It is important to note that updates provided by Red Hat may not be present on the system if the underlying packages are not installed.
Check that the available package security updates have been installed on the system with the following command:

```
$ dnf history list | more

    ID | Command line | Date and time | Action(s) | Altered
-------------------------------------------------------------------------------
--
   70 | install aide | 2023-03-05 10:58 | Install | 1
   69 | update -y | 2023-03-04 14:34 | Update | 18 EE
   68 | install vlc | 2023-02-21 17:12 | Install | 21
   67 | update -y | 2023-02-21 17:04 | Update | 7 EE
```

Typical update frequency may be overridden by Information Assurance Vulnerability Alert (IAVA) notifications from CYBERCOM.
If the system is in noncompliance with the organizational patching policy, this is a finding.

Remediation:

Install RHEL 9 security patches and updates at the organizationally defined frequency. If system updates are installed via a centralized repository that is configured on the system, all updates can be installed with the following command:

```
$ sudo dnf update
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.4 RHEL-09-211020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 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.

```
GROUP ID: V-257779
RULE ID: SV-257779r958390
```

Rationale:

Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via login interfaces with human users and are not required when such human interfaces do not exist.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000228-GPOS-00088

Audit:

Verify RHEL 9 displays the Standard Mandatory DOD Notice and Consent Banner before granting access to the operating system via a command line user logon.
Check that a banner is displayed at the command line login screen with the following command:
$ sudo cat /etc/issue
If the banner is set correctly it will return the following text:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent
to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC
monitoring, network operations and defense, personnel misconduct (PM), law
enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are
subject to routine monitoring, interception, and search, and may be disclosed
or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access
controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM,
LE or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or
services by attorneys, psychotherapists, or clergy, and their assistants.
Such communications and work product are private and confidential. See User
Agreement for details."

If the banner text does not match the Standard Mandatory DOD Notice and
Consent Banner exactly, or the line is commented out, this is a finding.
```

Remediation:

Configure RHEL 9 to display the Standard Mandatory DOD Notice and Consent Banner before granting access to the system via command line logon.
Edit the "/etc/issue" file to replace the default text with the Standard Mandatory DOD Notice and Consent Banner. The DOD-required text is:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent
to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC
monitoring, network operations and defense, personnel misconduct (PM), law
enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are
subject to routine monitoring, interception, and search, and may be disclosed
or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access
controls) to protect USG interests -- not for your personal benefit or
privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM,
LE or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or
services by attorneys, psychotherapists, or clergy, and their assistants.
Such communications and work product are private and confidential. See User
Agreement for details."
```

Additional Information:

CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53 :: AC-8 a
- NIST SP 800-53 Revision 4 :: AC-8 a
- NIST SP 800-53 Revision 5 :: AC-8 a
- NIST SP 800-53A :: AC-8.1 (ii)

CCI-001384 For publicly accessible systems, display system use information with organization-defined conditions before granting further access to the publicly accessible system.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 1
- NIST SP 800-53 Revision 5 :: AC-8 c 1
- NIST SP 800-53A :: AC-8.2 (i)

CCI-001385 For publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2
- NIST SP 800-53A :: AC-8.2 (ii)

CCI-001386 For publicly accessible systems, displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2
- NIST SP 800-53A :: AC-8.2 (ii)

CCI-001387 For publicly accessible systems, displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2
- NIST SP 800-53A :: AC-8.2 (ii)

CCI-001388 For publicly accessible systems, includes a description of the authorized uses of the system.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 3
- NIST SP 800-53 Revision 5 :: AC-8 c 3
- NIST SP 800-53A :: AC-8.2 (iii)

1.5 RHEL-09-211030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The graphical display manager must not be the default target on RHEL 9 unless approved.

```
GROUP ID: V-257781
RULE ID: SV-257781r991589
```

Rationale:

Unnecessary service packages must not be installed to decrease the attack surface of the system. Graphical display managers have a long history of security vulnerabilities and must not be used, unless approved and documented.

Audit:

Verify that RHEL 9 is configured to boot to the command line:

```
$ systemctl get-default

multi-user.target
```

If the system default target is not set to "multi-user.target" and the information system security officer (ISSO) lacks a documented requirement for a graphical user interface, this is a finding.

Remediation:

Document the requirement for a graphical user interface with the ISSO or set the default target to multi-user with the following command:

```
$ sudo systemctl set-default multi-user.target
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.6 RHEL-09-211035 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

RHEL 9 must enable the hardware random number generator entropy gatherer service.

```
GROUP ID: V-257782
RULE ID: SV-257782r991589
```

Rationale:

The most important characteristic of a random number generator is its randomness, namely its ability to deliver random numbers that are impossible to predict. Entropy in computer security is associated with the unpredictability of a source of randomness. The random source with high entropy tends to achieve a uniform distribution of random values. Random number generators are one of the most important building blocks of cryptosystems.

The rngd service feeds random data from hardware device to kernel random device. Quality (nonpredictable) random number generation is important for several security functions (i.e., ciphers).

Audit:

Note: For RHEL 9 systems running with kernel FIPS mode enabled as specified by RHEL-09-671010, this requirement is Not Applicable.
Verify that RHEL 9 has enabled the hardware random number generator entropy gatherer service with the following command:

```
$ systemctl is-active rngd

active
```

If the "rngd" service is not active, this is a finding.

Remediation:

Install the rng-tools package with the following command:

```
$ sudo dnf install rng-tools
```

Then enable the rngd service run the following command:

```
$ sudo systemctl enable --now rngd
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.7 RHEL-09-211040 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 systemd-journald service must be enabled.

```
GROUP ID: V-257783
RULE ID: SV-257783r991562
```

Rationale:

In the event of a system failure, RHEL 9 must preserve any information necessary to determine cause of failure and any information necessary to return to operations with least disruption to system processes.

Audit:

Verify that "systemd-journald" is active with the following command:

```
$ systemctl is-active systemd-journald

active
```

If the systemd-journald service is not active, this is a finding.

Remediation:

To enable the systemd-journald service, run the following command:

```
$ sudo systemctl enable --now systemd-journald
```

References:

1. CIS Recommendation: "Ensure journald service is enabled and active"

Additional Information:

CCI-001665 Preserve organization-defined system state information in the event of a system failure.

- NIST SP 800-53 :: SC-24
- NIST SP 800-53 Revision 4 :: SC-24
- NIST SP 800-53 Revision 5 :: SC-24
- NIST SP 800-53A :: SC-24.1 (v)

1.8 RHEL-09-211045 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

The systemd Ctrl-Alt-Delete burst key sequence in RHEL 9 must be disabled.

```
GROUP ID: V-257784
RULE ID: SV-257784r1044832
```

Rationale:

A locally logged-on user who presses Ctrl-Alt-Delete when at the console can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot. In a graphical user environment, risk of unintentional reboot from the Ctrl-Alt-Delete sequence is reduced because the user will be prompted before any action is taken.

Satisfies: SRG-OS-000324-GPOS-00125, SRG-OS-000480-GPOS-00227

Audit:

Verify RHEL 9 is configured to not reboot the system when Ctrl-Alt-Delete is pressed seven times within two seconds with the following command:

```
$ grep -i ctrl /etc/systemd/system.conf

CtrlAltDelBurstAction=none
```

If the "CtrlAltDelBurstAction" is not set to "none", commented out, or is missing, this is a finding.

Remediation:

Configure the system to disable the CtrlAltDelBurstAction by added or modifying the following line in the "/etc/systemd/system.conf" configuration file:

```
CtrlAltDelBurstAction=none
```

Reload the daemon for this change to take effect.

```
$ sudo systemctl daemon-reload
```

Additional Information:

CCI-002235 Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.9 RHEL-09-211050 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

The x86 Ctrl-Alt-Delete key sequence must be disabled on RHEL 9.

```
GROUP ID: V-257785
RULE ID: SV-257785r1044833
```

Rationale:

A locally logged-on user who presses Ctrl-Alt-Delete when at the console can reboot the system. If accidentally pressed, as could happen in the case of a mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot. In a graphical user environment, risk of unintentional reboot from the Ctrl-Alt-Delete sequence is reduced because the user will be prompted before any action is taken.

Satisfies: SRG-OS-000324-GPOS-00125, SRG-OS-000480-GPOS-00227

Audit:

Verify RHEL 9 is not configured to reboot the system when Ctrl-Alt-Delete is pressed with the following command:

```
$ sudo systemctl status ctrl-alt-del.target

ctrl-alt-del.target
Loaded: masked (Reason: Unit ctrl-alt-del.target is masked.)
Active: inactive (dead)
```

If the "ctrl-alt-del.target" is loaded and not masked, this is a finding.

Remediation:

Configure RHEL 9 to disable the ctrl-alt-del.target with the following command:

```
$ sudo systemctl disable --now ctrl-alt-del.target
$ sudo systemctl mask --now ctrl-alt-del.target
```

Additional Information:

CCI-002235 Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.10 RHEL-09-211055 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 debug-shell systemd service must be disabled.

```
GROUP ID: V-257786
RULE ID: SV-257786r1044834
```

Rationale:

The debug-shell requires no authentication and provides root privileges to anyone who has physical access to the machine. While this feature is disabled by default, masking it adds an additional layer of assurance that it will not be enabled via a dependency in systemd. This also prevents attackers with physical access from trivially bypassing security on the machine through valid troubleshooting configurations and gaining root access when the system is rebooted.

Satisfies: SRG-OS-000324-GPOS-00125, SRG-OS-000480-GPOS-00227

Audit:

Verify RHEL 9 is configured to mask the debug-shell systemd service with the following command:

```
$ sudo systemctl status debug-shell.service

debug-shell.service
Loaded: masked (Reason: Unit debug-shell.service is masked.)
Active: inactive (dead)
```

If the "debug-shell.service" is loaded and not masked, this is a finding.

Remediation:

Configure RHEL 9 to mask the debug-shell systemd service with the following command:

```
$ sudo systemctl disable --now debug-shell.service
$ sudo systemctl mask --now debug-shell.service
```

Additional Information:

CCI-002235 Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.11 RHEL-09-212010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must require a boot loader superuser password.

```
GROUP ID: V-257787
RULE ID: SV-257787r1044836
```

Rationale:

To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DOD-approved PKIs, all DOD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

Password protection on the boot loader configuration ensures users with physical access cannot trivially alter important bootloader settings. These include which kernel to use, and whether to enter single-user mode.

Audit:

Verify the boot loader superuser password has been set with the following command:

```
$ sudo grep password_pbkdf2 /etc/grub2.cfg

password_pbkdf2  <superusers-accountname>   ${GRUB2_PASSWORD}
```

To verify the boot loader superuser account password has been set and the password encrypted, run the following command:

```
$ sudo cat /boot/grub2/user.cfg

GRUB2_PASSWORD=grub.pbkdf2.sha512.10000.C4E08AC72FBFF7E837FD267BFAD7AEB3D42DD
C
2C99F2A94DD5E2E75C2DC331B719FE55D9411745F82D1B6CFD9E927D61925F9BBDD1CFAA0080E
0
916F7AB46E0D.1302284FCCC52CD73BA3671C6C12C26FF50BA873293B24EE2A96EE3B57963E6D
7
0C83964B473EC8F93B07FE749AA6710269E904A9B08A6BBACB00A2D242AD828
```

If a "GRUB2_PASSWORD" is not set, this is a finding.

Remediation:

Configure RHEL 9 to require a grub bootloader password for the grub superuser account.
Generate an encrypted grub2 password for the grub superuser account with the following command:

```
$ sudo grub2-setpassword
Enter password:
Confirm password:
```

References:

1. CIS Recommendation: "Ensure bootloader password is set"

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53 :: AC-3
- NIST SP 800-53 Revision 4 :: AC-3
- NIST SP 800-53 Revision 5 :: AC-3
- NIST SP 800-53A :: AC-3.1

1.12 RHEL-09-212015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must disable the ability of systemd to spawn an interactive boot process.

```
GROUP ID: V-257788
RULE ID: SV-257788r1044838
```

Rationale:

Using interactive or recovery boot, the console user could disable auditing, firewalls, or other services, weakening system security.

Audit:

Verify that GRUB 2 is configured to disable interactive boot.
Check that the current GRUB 2 configuration disables the ability of systemd to spawn an interactive boot process with the following command:

```
$ sudo grubby --info=ALL | grep args | grep 'systemd.confirm_spawn'
```

If any output is returned, this is a finding.

Remediation:

Configure the current GRUB 2 configuration to disable the ability of systemd to spawn an interactive boot process with the following command:

```
$ sudo grubby --update-kernel=ALL --remove-args="systemd.confirm_spawn"
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.13 RHEL-09-212020 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

RHEL 9 must require a unique superusers name upon booting into single-user and maintenance modes.

```
GROUP ID: V-257789
RULE ID: SV-257789r1069356
```

Rationale:

Having a nondefault grub superuser username makes password-guessing attacks less effective.

Audit:

Verify the boot loader superuser account has been set with the following command:

```
$ sudo grep -A1 "superusers" /etc/grub2.cfg

set superusers="<accountname>"
export superusers
password_pbkdf2 <accountname> ${GRUB2_PASSWORD}
```

Verify is not a common name such as root, admin, or administrator.
If superusers contains easily guessable usernames, this is a finding.

Remediation:

Configure RHEL 9 to have a unique username for the grub superuser account.
Edit the "/etc/grub.d/01_users" file and add or modify the following lines with a nondefault username for the superuser account:

```
set superusers="<accountname>"
export superusers
```

Once the superuser account has been added, update the grub.cfg file by running:
Regenerate the GRUB configuration:

```
$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

Reboot the system:

```
$ sudo reboot
```

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53 :: AC-3
- NIST SP 800-53 Revision 4 :: AC-3
- NIST SP 800-53 Revision 5 :: AC-3
- NIST SP 800-53A :: AC-3.1

1.14 RHEL-09-212025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /boot/grub2/grub.cfg file must be group-owned by root.

```
GROUP ID: V-257790
RULE ID: SV-257790r991589
```

Rationale:

The "root" group is a highly privileged group. Furthermore, the group-owner of this file should not have any access privileges anyway.

Audit:

Verify the group ownership of the "/boot/grub2/grub.cfg" file with the following command:

```
$ sudo stat -c "%G %n" /boot/grub2/grub.cfg

root /boot/grub2/grub.cfg
```

If "/boot/grub2/grub.cfg" file does not have a group owner of "root", this is a finding.

Remediation:

Change the group of the file /boot/grub2/grub.cfg to root by running the following command:

```
$ sudo chgrp root /boot/grub2/grub.cfg
```

References:

1. CIS Recommendation: "Ensure access to bootloader config is configured"

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.15 RHEL-09-212030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /boot/grub2/grub.cfg file must be owned by root.

```
GROUP ID: V-257791
RULE ID: SV-257791r991589
```

Rationale:

The " /boot/grub2/grub.cfg" file stores sensitive system configuration. Protection of this file is critical for system security.

Audit:

Verify the ownership of the "/boot/grub2/grub.cfg" file with the following command:

```
$ sudo stat -c "%U %n" /boot/grub2/grub.cfg

root /boot/grub2/grub.cfg
```

If "/boot/grub2/grub.cfg" file does not have an owner of "root", this is a finding.

Remediation:

Change the owner of the file /boot/grub2/grub.cfg to root by running the following command:

```
$ sudo chown root /boot/grub2/grub.cfg
```

References:

1. CIS Recommendation: "Ensure access to bootloader config is configured"

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.16 RHEL-09-212035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must disable virtual system calls.

```
GROUP ID: V-257792
RULE ID: SV-257792r1044842
```

Rationale:

System calls are special routines in the Linux kernel, which userspace applications ask to do privileged tasks. Invoking a system call is an expensive operation because the processor must interrupt the currently executing task and switch context to kernel mode and then back to userspace after the system call completes. Virtual system calls map into user space a page that contains some variables and the implementation of some system calls. This allows the system calls to be executed in userspace to alleviate the context switching expense.

Virtual system calls provide an opportunity of attack for a user who has control of the return instruction pointer. Disabling virtual system calls help to prevent return oriented programming (ROP) attacks via buffer overflows and overruns. If the system intends to run containers based on RHEL 6 components, then virtual system calls will need enabled so the components function properly.

Satisfies: SRG-OS-000480-GPOS-00227, SRG-OS-000134-GPOS-00068

Audit:

Verify the current GRUB 2 configuration disables virtual system calls with the following command:

```
$ sudo grubby --info=ALL | grep args | grep -v 'vsyscall=none'
```

If any output is returned, this is a finding.
Check that virtual system calls are disabled by default to persist in kernel updates with the following command:

```
$ sudo grep vsyscall /etc/default/grub

GRUB_CMDLINE_LINUX="vsyscall=none"
```

If "vsyscall" is not set to "none", is missing or commented out, and is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Document the use of virtual system calls with the ISSO as an operational requirement or disable them with the following command:

```
$ sudo grubby --update-kernel=ALL --args="vsyscall=none"
```

Add or modify the following line in "/etc/default/grub" to ensure the configuration survives kernel updates:

```
GRUB_CMDLINE_LINUX="vsyscall=none"
```

Additional Information:

CCI-001084 Isolate security functions from nonsecurity functions.

- NIST SP 800-53 :: SC-3
- NIST SP 800-53 Revision 4 :: SC-3
- NIST SP 800-53 Revision 5 :: SC-3
- NIST SP 800-53A :: SC-3.1 (ii)

1.17 RHEL-09-212040 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must clear the page allocator to prevent use-after-free attacks.

```
GROUP ID: V-257793
RULE ID: SV-257793r1044843
```

Rationale:

Poisoning writes an arbitrary value to freed pages, so any modification or reference to that page after being freed or before being initialized will be detected and prevented. This prevents many types of use-after-free vulnerabilities at little performance cost. Also prevents leak of data and detection of corrupted memory.

Satisfies: SRG-OS-000480-GPOS-00227, SRG-OS-000134-GPOS-00068

Audit:

Verify that GRUB 2 is configured to enable page poisoning to mitigate use-after-free vulnerabilities.
Check that the current GRUB 2 configuration has page poisoning enabled with the following command:

```
$ sudo grubby --info=ALL | grep args | grep -v 'page_poison=1'
```

If any output is returned, this is a finding.
Check that page poisoning is enabled by default to persist in kernel updates with the following command:

```
$ sudo grep page_poison /etc/default/grub

GRUB_CMDLINE_LINUX="page_poison=1"
```

If "page_poison" is not set to "1", is missing or commented out, this is a finding.

Remediation:

Configure RHEL 9 to enable page poisoning with the following commands:

```
$ sudo grubby --update-kernel=ALL --args="page_poison=1"
```

Add or modify the following line in "/etc/default/grub" to ensure the configuration survives kernel updates:

```
GRUB_CMDLINE_LINUX="page_poison=1"
```

Additional Information:

CCI-001084 Isolate security functions from nonsecurity functions.

- NIST SP 800-53 :: SC-3
- NIST SP 800-53 Revision 4 :: SC-3
- NIST SP 800-53 Revision 5 :: SC-3
- NIST SP 800-53A :: SC-3.1 (ii)

1.18 RHEL-09-212045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must clear memory when it is freed to prevent use-after-free attacks.

```
GROUP ID: V-257794
RULE ID: SV-257794r1069362
```

Rationale:

Some adversaries launch attacks with the intent of executing code in nonexecutable regions of memory or in memory locations that are prohibited. Security safeguards employed to protect memory include, for example, data execution prevention and address space layout randomization. Data execution prevention safeguards can be either hardware-enforced or software-enforced with hardware providing the greater strength of mechanism.

Poisoning writes an arbitrary value to freed pages, so any modification or reference to that page after being freed or before being initialized will be detected and prevented. This prevents many types of use-after-free vulnerabilities at little performance cost. Also prevents leak of data and detection of corrupted memory.

init_on_free is a Linux kernel boot parameter that enhances security by initializing memory regions when they are freed, preventing data leakage. This process ensures that stale data in freed memory cannot be accessed by malicious programs.

SLUB canaries add a randomized value (canary) at the end of SLUB-allocated objects to detect memory corruption caused by buffer overflows or underflows. Redzoning adds padding (red zones) around SLUB-allocated objects to detect overflows or underflows by triggering a fault when adjacent memory is accessed. SLUB canaries are often more efficient and provide stronger detection against buffer overflows compared to redzoning. SLUB canaries are supported in hardened Linux kernels like the ones provided by Linux-hardened.

SLAB objects are blocks of physically contiguous memory. SLUB is the unqueued SLAB allocator.

Satisfies: SRG-OS-000433-GPOS-00192, SRG-OS-000134-GPOS-00068

Audit:

Verify that GRUB2 is configured to mitigate use-after-free vulnerabilities by employing memory poisoning.
Inspect the "GRUB_CMDLINE_LINUX" entry of /etc/default/grub as follows:

```
$ sudo grep -i grub_cmdline_linux /etc/default/grub

GRUB_CMDLINE_LINUX="... init_on_free=1"
```

If "init_on_free=1" is missing or commented out, this is a finding.

Remediation:

Configure RHEL 9 to enable init_on_free with the following command:

```
$ sudo grubby --update-kernel=ALL --args="init_on_free=1"
```

Regenerate the GRUB configuration:

```
$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

Reboot the system:

```
$ sudo reboot
```

Additional Information:

CCI-001084 Isolate security functions from nonsecurity functions.

- NIST SP 800-53 :: SC-3
- NIST SP 800-53 Revision 4 :: SC-3
- NIST SP 800-53 Revision 5 :: SC-3
- NIST SP 800-53A :: SC-3.1 (ii)

CCI-002824 Implement organization-defined controls to protect its memory from unauthorized code execution.

- NIST SP 800-53 Revision 4 :: SI-16
- NIST SP 800-53 Revision 5 :: SI-16

1.19 RHEL-09-212050 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

RHEL 9 must enable mitigations against processor-based vulnerabilities.

```
GROUP ID: V-257795
RULE ID: SV-257795r1044845
```

Rationale:

Kernel page-table isolation is a kernel feature that mitigates the Meltdown security vulnerability and hardens the kernel against attempts to bypass kernel address space layout randomization (KASLR).

Satisfies: SRG-OS-000433-GPOS-00193, SRG-OS-000095-GPOS-00049

Audit:

Verify RHEL 9 enables kernel page-table isolation with the following command:

```
$ sudo grubby --info=ALL | grep args | grep -v 'pti=on'
```

If any output is returned, this is a finding.
Check that kernel page-table isolation is enabled by default to persist in kernel updates:

```
$ grep pti /etc/default/grub

GRUB_CMDLINE_LINUX="pti=on"
```

If "pti" is not set to "on", is missing or commented out, this is a finding.

Remediation:

Configure RHEL 9 to enable kernel page-table isolation with the following command:

```
$ sudo grubby --update-kernel=ALL --args="pti=on"
```

Add or modify the following line in "/etc/default/grub" to ensure the configuration survives kernel updates:

```
GRUB_CMDLINE_LINUX="pti=on"
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

CCI-002824 Implement organization-defined controls to protect its memory from unauthorized code execution.

- NIST SP 800-53 Revision 4 :: SI-16
- NIST SP 800-53 Revision 5 :: SI-16

1.20 RHEL-09-212055 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

RHEL 9 must enable auditing of processes that start prior to the audit daemon.

```
GROUP ID: V-257796
RULE ID: SV-257796r1044847
```

Rationale:

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

If auditing is enabled late in the startup process, the actions of some startup processes may not be audited. Some audit systems also maintain state information only available if auditing is enabled before a given process is created.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000473-GPOS-00218, SRG-OS-000254-GPOS-00095

Audit:

Verify that GRUB 2 is configured to enable auditing of processes that start prior to the audit daemon with the following commands:
Check that the current GRUB 2 configuration enables auditing:

```
$ sudo grubby --info=ALL | grep args | grep -v 'audit=1'
```

If any output is returned, this is a finding.
Check that auditing is enabled by default to persist in kernel updates:

```
$ grep audit /etc/default/grub

GRUB_CMDLINE_LINUX="audit=1"
```

If "audit" is not set to "1", is missing, or is commented out, this is a finding.

Remediation:

Enable auditing of processes that start prior to the audit daemon with the following command:

```
$ sudo grubby --update-kernel=ALL --args="audit=1"
```

Add or modify the following line in "/etc/default/grub" to ensure the configuration survives kernel updates:

```
GRUB_CMDLINE_LINUX="audit=1"
```

References:

1. CIS Recommendation: "Ensure auditing for processes that start prior to auditd is enabled"

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-001464 Initiates session audits automatically at system start-up.

- NIST SP 800-53 :: AU-14 (1)
- NIST SP 800-53 Revision 4 :: AU-14 (1)
- NIST SP 800-53 Revision 5 :: AU-14 (1)
- NIST SP 800-53A :: AU-14 (1).1

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.21 RHEL-09-213010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must restrict access to the kernel message buffer.

```
GROUP ID: V-257797
RULE ID: SV-257797r958514
```

Rationale:

Preventing unauthorized information transfers mitigates the risk of information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection.

This requirement generally applies to the design of an information technology product, but it can also apply to the configuration of particular information system components that are, or use, such products. This can be verified by acceptance/validation processes in DOD or other government agencies.

There may be shared resources with configurable protections (e.g., files in storage) that may be assessed on specific information system components.

Restricting access to the kernel message buffer limits access to only root. This prevents attackers from gaining additional system information as a nonprivileged user.

Satisfies: SRG-OS-000132-GPOS-00067, SRG-OS-000138-GPOS-00069

Audit:

Verify RHEL 9 is configured to restrict access to the kernel message buffer with the following commands:
Check the status of the kernel.dmesg_restrict kernel parameter.

```
$ sudo sysctl kernel.dmesg_restrict

kernel.dmesg_restrict = 1
```

If "kernel.dmesg_restrict" is not set to "1" or is missing, this is a finding.
Check that the configuration files are present to enable this kernel parameter.
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' | grep -F kernel.dmesg_restrict | tail -1

```
kernel.dmesg_restrict = 1
```

If "kernel.dmesg_restrict" is not set to "1" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to restrict access to the kernel message buffer.
Add or edit the following line in a system configuration file, in the "/etc/sysctl.d/" directory:

```
kernel.dmesg_restrict = 1
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-001082 Separate user functionality, including user interface services, from system management functionality.

- NIST SP 800-53 :: SC-2
- NIST SP 800-53 Revision 4 :: SC-2
- NIST SP 800-53 Revision 5 :: SC-2
- NIST SP 800-53A :: SC-2.1

CCI-001090 Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53 :: SC-4
- NIST SP 800-53 Revision 4 :: SC-4
- NIST SP 800-53 Revision 5 :: SC-4
- NIST SP 800-53A :: SC-4.1

1.22 RHEL-09-213015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent kernel profiling by nonprivileged users.

```
GROUP ID: V-257798
RULE ID: SV-257798r1044849
```

Rationale:

Preventing unauthorized information transfers mitigates the risk of information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection.

This requirement generally applies to the design of an information technology product, but it can also apply to the configuration of particular information system components that are, or use, such products. This can be verified by acceptance/validation processes in DOD or other government agencies.

There may be shared resources with configurable protections (e.g., files in storage) that may be assessed on specific information system components.

Setting the kernel.perf_event_paranoid kernel parameter to "2" prevents attackers from gaining additional system information as a nonprivileged user.

Satisfies: SRG-OS-000132-GPOS-00067, SRG-OS-000138-GPOS-00069

Audit:

Verify RHEL 9 is configured to prevent kernel profiling by nonprivileged users with the following commands:
Check the status of the kernel.perf_event_paranoid kernel parameter.

```
$ sysctl kernel.perf_event_paranoid

kernel.perf_event_paranoid = 2
```

If "kernel.perf_event_paranoid" is not set to "2" or is missing, this is a finding.
Check that the configuration files are present to enable this kernel parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config  | egrep -v '^(#|;)' |
grep -F kernel.perf_event_paranoid | tail -1

kernel.perf_event_paranoid = 2
```

If "kernel.perf_event_paranoid" is not set to "2" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to prevent kernel profiling by nonprivileged users.
Add or edit the following line in a system configuration file, in the "/etc/sysctl.d/" directory:

```
kernel.perf_event_paranoid = 2
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-001082 Separate user functionality, including user interface services, from system management functionality.

- NIST SP 800-53 :: SC-2
- NIST SP 800-53 Revision 4 :: SC-2
- NIST SP 800-53 Revision 5 :: SC-2
- NIST SP 800-53A :: SC-2.1

CCI-001090 Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53 :: SC-4
- NIST SP 800-53 Revision 4 :: SC-4
- NIST SP 800-53 Revision 5 :: SC-4
- NIST SP 800-53A :: SC-4.1

1.23 RHEL-09-213020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent the loading of a new kernel for later execution.

```
GROUP ID: V-257799
RULE ID: SV-257799r1044850
```

Rationale:

Changes to any software components can have significant effects on the overall security of the operating system. This requirement ensures the software has not been tampered with and that it has been provided by a trusted vendor.

Disabling kexec_load prevents an unsigned kernel image (that could be a windows kernel or modified vulnerable kernel) from being loaded. Kexec can be used subvert the entire secureboot process and should be avoided at all costs especially since it can load unsigned kernel images.

Satisfies: SRG-OS-000480-GPOS-00227, SRG-OS-000366-GPOS-00153

Audit:

Verify RHEL 9 is configured to disable kernel image loading.
Check the status of the kernel.kexec_load_disabled kernel parameter with the following command:

```
$ sudo sysctl kernel.kexec_load_disabled

kernel.kexec_load_disabled = 1
```

If "kernel.kexec_load_disabled" is not set to "1" or is missing, this is a finding.
Check that the configuration files are present to enable this kernel parameter with the following command:

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F kernel.kexec_load_disabled | tail -1

kernel.kexec_load_disabled = 1
```

If "kernel.kexec_load_disabled" is not set to "1" or is missing, this is a finding.

Remediation:

Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory:

```
kernel.kexec_load_disabled = 1
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5 :: CM-14

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.

- NIST SP 800-53 Revision 4 :: CM-5 (3)

1.24 RHEL-09-213025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must restrict exposed kernel pointer addresses access.

```
GROUP ID: V-257800
RULE ID: SV-257800r1044851
```

Rationale:

Exposing kernel pointers (through procfs or "seq_printf()") exposes kernel writeable structures, which may contain functions pointers. If a write vulnerability occurs in the kernel, allowing write access to any of this structure, the kernel can be compromised. This option disallows any program without the CAP_SYSLOG capability to get the addresses of kernel pointers by replacing them with "0".

Satisfies: SRG-OS-000132-GPOS-00067, SRG-OS-000433-GPOS-00192, SRG-OS-000480-GPOS-00227

Audit:

Verify the runtime status of the kernel.kptr_restrict kernel parameter with the following command:

```
$ sudo sysctl kernel.kptr_restrict

kernel.kptr_restrict = 1
```

Verify the configuration of the kernel.kptr_restrict kernel parameter with the following command:

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F kernel.kptr_restrict | tail -1

kernel.kptr_restrict =1
```

If "kernel.kptr_restrict" is not set to "1" or is missing, this is a finding.

Remediation:

Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory:

```
kernel.kptr_restrict = 1
```

Reload settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-001082 Separate user functionality, including user interface services, from system management functionality.

- NIST SP 800-53 :: SC-2
- NIST SP 800-53 Revision 4 :: SC-2
- NIST SP 800-53 Revision 5 :: SC-2
- NIST SP 800-53A :: SC-2.1

CCI-002824 Implement organization-defined controls to protect its memory from unauthorized code execution.

- NIST SP 800-53 Revision 4 :: SI-16
- NIST SP 800-53 Revision 5 :: SI-16

1.25 RHEL-09-213030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must enable kernel parameters to enforce discretionary access control on hardlinks.

```
GROUP ID: V-257801
RULE ID: SV-257801r958702
```

Rationale:

By enabling the fs.protected_hardlinks kernel parameter, users can no longer create soft or hard links to files they do not own. Disallowing such hardlinks mitigates vulnerabilities based on insecure file system accessed by privileged programs, avoiding an exploitation vector exploiting unsafe use of open() or creat().

Satisfies: SRG-OS-000312-GPOS-00123, SRG-OS-000324-GPOS-00125

Audit:

Verify RHEL 9 is configured to enable DAC on hardlinks.
Check the status of the fs.protected_hardlinks kernel parameter with the following command:

```
$ sudo sysctl fs.protected_hardlinks

fs.protected_hardlinks = 1
```

If "fs.protected_hardlinks" is not set to "1" or is missing, this is a finding.
Check that the configuration files are present to enable this kernel parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F fs.protected_hardlinks | tail -1

fs.protected_hardlinks = 1
```

If "fs.protected_hardlinks" is not set to "1" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to enable DAC on hardlinks with the following:
Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory:

```
fs.protected_hardlinks = 1
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-002165 Enforce organization-defined discretionary access control policies over defined subjects and objects.

- NIST SP 800-53 Revision 4 :: AC-3 (4)
- NIST SP 800-53 Revision 5 :: AC-3 (4)

CCI-002235 Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.26 RHEL-09-213035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must enable kernel parameters to enforce discretionary access control on symlinks.

```
GROUP ID: V-257802
RULE ID: SV-257802r958702
```

Rationale:

By enabling the fs.protected_symlinks kernel parameter, symbolic links are permitted to be followed only when outside a sticky world-writable directory, or when the user identifier (UID) of the link and follower match, or when the directory owner matches the symlink's owner. Disallowing such symlinks helps mitigate vulnerabilities based on insecure file system accessed by privileged programs, avoiding an exploitation vector exploiting unsafe use of open() or creat().

Satisfies: SRG-OS-000312-GPOS-00123, SRG-OS-000324-GPOS-00125

Audit:

Verify RHEL 9 is configured to enable DAC on symlinks.
Check the status of the fs.protected_symlinks kernel parameter with the following command:

```
$ sudo sysctl fs.protected_symlinks

fs.protected_symlinks = 1
```

If "fs.protected_symlinks " is not set to "1" or is missing, this is a finding.
Check that the configuration files are present to enable this kernel parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F fs.protected_symlinks | tail -1

fs.protected_symlinks = 1
```

If "fs.protected_symlinks" is not set to "1" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to enable DAC on symlinks with the following:
Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory:

```
fs.protected_symlinks = 1
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-002165 Enforce organization-defined discretionary access control policies over defined subjects and objects.

- NIST SP 800-53 Revision 4 :: AC-3 (4)
- NIST SP 800-53 Revision 5 :: AC-3 (4)

CCI-002235 Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.27 RHEL-09-213040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must disable the kernel.core_pattern.

```
GROUP ID: V-257803
RULE ID: SV-257803r991589
```

Rationale:

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems.

Audit:

Verify RHEL 9 disables storing core dumps with the following commands:

```
$ sudo sysctl kernel.core_pattern

kernel.core_pattern = |/bin/false
```

If the returned line does not have a value of "|/bin/false", or a line is not returned and the need for core dumps is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.
Check that the configuration files are present to disable core dump storage.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F kernel.core_pattern | tail -1

kernel.core_pattern = |/bin/false
```

If "kernel.core_pattern" is not set to "|/bin/false" and is not documented with the ISSO as an operational requirement, or is missing, this is a finding.

Remediation:

Configure RHEL 9 to disable storing core dumps.
Add or edit the following line in a system configuration file, in the "/etc/sysctl.d/" directory:

```
kernel.core_pattern = |/bin/false
```

The system configuration files need to be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.28 RHEL-09-213045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must be configured to disable the Asynchronous Transfer Mode kernel module.

```
GROUP ID: V-257804
RULE ID: SV-257804r1044853
```

Rationale:

Disabling Asynchronous Transfer Mode (ATM) protects the system against exploitation of any flaws in its implementation.

Audit:

Verify that RHEL 9 disables the ability to load the ATM kernel module with the following command:

```
$ grep -r atm /etc/modprobe.conf /etc/modprobe.d/*

install atm /bin/false
blacklist atm
```

If the command does not return any output, or the line is commented out, and use of ATM is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Remediation:

To configure the system to prevent the atm kernel module from being loaded, add the following line to the file /etc/modprobe.d/atm.conf (or create atm.conf if it does not exist):

```
install atm /bin/false
blacklist atm
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.29 RHEL-09-213050 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must be configured to disable the Controller Area Network kernel module.

```
GROUP ID: V-257805
RULE ID: SV-257805r1044856
```

Rationale:

Disabling Controller Area Network (CAN) protects the system against exploitation of any flaws in its implementation.

Audit:

Verify that RHEL 9 disables the ability to load the CAN kernel module with the following command:

```
$ grep -r can /etc/modprobe.conf /etc/modprobe.d/*

install can /bin/false
blacklist can
```

If the command does not return any output, or the lines are commented out, and use of CAN is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Remediation:

To configure the system to prevent the can kernel module from being loaded, add the following lines to the file /etc/modprobe.d/can.conf (or create can.conf if it does not exist):

```
install can /bin/false
blacklist can
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.30 RHEL-09-213055 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must be configured to disable the FireWire kernel module.

```
GROUP ID: V-257806
RULE ID: SV-257806r1044859
```

Rationale:

Disabling firewire protects the system against exploitation of any flaws in its implementation.

Audit:

Verify that RHEL 9 disables the ability to load the firewire-core kernel module with the following command:

```
$ grep -r firewire-core /etc/modprobe.conf /etc/modprobe.d/*

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

If the command does not return any output, or the lines are commented out, and use of firewire-core is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Remediation:

To configure the system to prevent the firewire-core kernel module from being loaded, add the following lines to the file /etc/modprobe.d/firewire-core.conf (or create firewire-core.conf if it does not exist):

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

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.31 RHEL-09-213060 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must disable the Stream Control Transmission Protocol (SCTP) kernel module.

```
GROUP ID: V-257807
RULE ID: SV-257807r1044862
```

Rationale:

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

Failing to disconnect unused protocols can result in a system compromise.

The Stream Control Transmission Protocol (SCTP) is a transport layer protocol, designed to support the idea of message-oriented communication, with several streams of messages within one connection. Disabling SCTP protects the system against exploitation of any flaws in its implementation.

Audit:

Verify that RHEL 9 disables the ability to load the sctp kernel module with the following command:

```
$ grep -r sctp /etc/modprobe.conf /etc/modprobe.d/*

install sctp /bin/false
blacklist sctp
```

If the command does not return any output, or the lines are commented out, and use of sctp is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Remediation:

To configure the system to prevent the sctp kernel module from being loaded, add the following lines to the file /etc/modprobe.d/sctp.conf (or create sctp.conf if it does not exist):

```
install sctp /bin/false
blacklist sctp
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.32 RHEL-09-213065 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must disable the Transparent Inter Process Communication (TIPC) kernel module.

```
GROUP ID: V-257808
RULE ID: SV-257808r1044865
```

Rationale:

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

Failing to disconnect unused protocols can result in a system compromise.

The Transparent Inter Process Communication (TIPC) is a protocol that is specially designed for intra-cluster communication. It can be configured to transmit messages either on UDP or directly across Ethernet. Message delivery is sequence guaranteed, loss free and flow controlled. Disabling TIPC protects the system against exploitation of any flaws in its implementation.

Audit:

Verify that RHEL 9 disables the ability to load the tipc kernel module with the following command:

```
$ grep -r tipc /etc/modprobe.conf /etc/modprobe.d/*

install tipc /bin/false
blacklist tipc
```

If the command does not return any output, or the lines are commented out, and use of tipc is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Remediation:

To configure the system to prevent the tipc kernel module from being loaded, add the following lines to the file /etc/modprobe.d/tipc.conf (or create tipc.conf if it does not exist):

```
install tipc /bin/false
blacklist tipc
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.33 RHEL-09-213070 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must implement address space layout randomization (ASLR) to protect its memory from unauthorized code execution.

```
GROUP ID: V-257809
RULE ID: SV-257809r1044866
```

Rationale:

Address space layout randomization (ASLR) makes it more difficult for an attacker to predict the location of attack code they have introduced into a process' address space during an attempt at exploitation. Additionally, ASLR makes it more difficult for an attacker to know the location of existing code in order to repurpose it using return oriented programming (ROP) techniques.

Satisfies: SRG-OS-000433-GPOS-00193, SRG-OS-000480-GPOS-00227

Audit:

Verify RHEL 9 is implementing ASLR with the following command:

```
$ sudo sysctl kernel.randomize_va_space

kernel.randomize_va_space = 2
```

Check that the configuration files are present to enable this kernel parameter.
Verify the configuration of the kernel.kptr_restrict kernel parameter with the following command:

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F kernel.randomize_va_space | tail -1

kernel.randomize_va_space = 2
```

If "kernel.randomize_va_space" is not set to "2" or is missing, this is a finding.

Remediation:

Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory:

```
kernel.randomize_va_space = 2
```

Reload settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-002824 Implement organization-defined controls to protect its memory from unauthorized code execution.

- NIST SP 800-53 Revision 4 :: SI-16
- NIST SP 800-53 Revision 5 :: SI-16

1.34 RHEL-09-213075 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must disable access to network bpf system call from nonprivileged processes.

```
GROUP ID: V-257810
RULE ID: SV-257810r1044869
```

Rationale:

Loading and accessing the packet filters programs and maps using the bpf() system call has the potential of revealing sensitive information about the kernel state.

Satisfies: SRG-OS-000132-GPOS-00067, SRG-OS-000480-GPOS-00227

Audit:

Verify that RHEL 9 prevents privilege escalation through the kernel by disabling access to the bpf system call with the following commands:

```
$ sysctl kernel.unprivileged_bpf_disabled

kernel.unprivileged_bpf_disabled = 1
```

If the returned line does not have a value of "1", or a line is not returned, this is a finding.
Check that the configuration files are present to enable this kernel parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F kernel.unprivileged_bpf_disabled | tail -1

kernel.unprivileged_bpf_disabled = 1
```

If the network parameter "kernel.unprivileged_bpf_disabled" is not equal to "1", or nothing is returned, this is a finding.

Remediation:

Configure the currently loaded kernel parameter to the secure setting:

```
$ sudo sysctl -w kernel.unprivileged_bpf_disabled=1
```

Configure RHEL 9 to prevent privilege escalation through the kernel by disabling access to the bpf syscall by adding the following line to a file in the "/etc/sysctl.d" directory:

```
kernel.unprivileged_bpf_disabled = 1
```

The system configuration files must be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
$ sysctl --system
```

Additional Information:

CCI-001082 Separate user functionality, including user interface services, from system management functionality.

- NIST SP 800-53 :: SC-2
- NIST SP 800-53 Revision 4 :: SC-2
- NIST SP 800-53 Revision 5 :: SC-2
- NIST SP 800-53A :: SC-2.1

1.35 RHEL-09-213080 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must restrict usage of ptrace to descendant processes.

```
GROUP ID: V-257811
RULE ID: SV-257811r1044872
```

Rationale:

Unrestricted usage of ptrace allows compromised binaries to run ptrace on other processes of the user. Like this, the attacker can steal sensitive information from the target processes (e.g., SSH sessions, web browser, etc.) without any additional assistance from the user (i.e., without resorting to phishing).

Satisfies: SRG-OS-000132-GPOS-00067, SRG-OS-000480-GPOS-00227

Audit:

Verify RHEL 9 restricts the usage of ptrace to descendant processes with the following commands:

```
$ sysctl kernel.yama.ptrace_scope

kernel.yama.ptrace_scope = 1
```

If the returned line does not have a value of "1", or a line is not returned, this is a finding.
Check that the configuration files are present to enable this kernel parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F kernel.yama.ptrace_scope| tail -1

kernel.yama.ptrace_scope = 1
```

If the network parameter "kernel.yama.ptrace_scope" is not equal to "1", or nothing is returned, this is a finding.

Remediation:

Configure the currently loaded kernel parameter to the secure setting:

```
$ sudo sysctl -w kernel.yama.ptrace_scope=1
```

Configure RHEL 9 to restrict usage of ptrace to descendant processes by adding the following line to a file in the "/etc/sysctl.d" directory:

```
kernel.yama.ptrace_scope = 1
```

The system configuration files must be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
$ sysctl --system
```

Additional Information:

CCI-001082 Separate user functionality, including user interface services, from system management functionality.

- NIST SP 800-53 :: SC-2
- NIST SP 800-53 Revision 4 :: SC-2
- NIST SP 800-53 Revision 5 :: SC-2
- NIST SP 800-53A :: SC-2.1

1.36 RHEL-09-213085 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must disable core dump backtraces.

```
GROUP ID: V-257812
RULE ID: SV-257812r1051005
```

Rationale:

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers or system operators trying to debug problems.

Enabling core dumps on production systems is not recommended; however, there may be overriding operational requirements to enable advanced debugging. Permitting temporary enablement of core dumps during such situations must be reviewed through local needs and policy.

Audit:

Verify RHEL 9 disables core dump backtraces by issuing the following command:

```
$ grep -i ProcessSizeMax /etc/systemd/coredump.conf

ProcessSizeMax=0
```

If the "ProcessSizeMax" item is missing or commented out, or the value is anything other than "0", and the need for core dumps is not documented with the information system security officer (ISSO) as an operational requirement for all domains that have the "core" item assigned, this is a finding.

Remediation:

Configure the operating system to disable core dump backtraces.
Add or modify the following line in /etc/systemd/coredump.conf:

```
ProcessSizeMax=0
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.37 RHEL-09-213090 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must disable storing core dumps.

```
GROUP ID: V-257813
RULE ID: SV-257813r991589
```

Rationale:

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers or system operators trying to debug problems. Enabling core dumps on production systems is not recommended; however, there may be overriding operational requirements to enable advanced debugging. Permitting temporary enablement of core dumps during such situations must be reviewed through local needs and policy.

Audit:

Verify RHEL 9 disables storing core dumps for all users by issuing the following command:

```
$ grep -i storage /etc/systemd/coredump.conf

Storage=none
```

If the "Storage" item is missing, commented out, or the value is anything other than "none" and the need for core dumps is not documented with the information system security officer (ISSO) as an operational requirement for all domains that have the "core" item assigned, this is a finding.

Remediation:

Configure the operating system to disable storing core dumps for all users.
Add or modify the following line in /etc/systemd/coredump.conf:

```
Storage=none
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.38 RHEL-09-213095 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must disable core dumps for all users.

```
GROUP ID: V-257814
RULE ID: SV-257814r991589
```

Rationale:

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems.

Audit:

Verify RHEL 9 disables core dumps for all users by issuing the following command:

```
$ grep -r -s core /etc/security/limits.conf /etc/security/limits.d/*.conf

/etc/security/limits.conf:* hard core 0
```

This can be set as a global domain (with the * wildcard) but may be set differently for multiple domains.
If the "core" item is missing, commented out, or the value is anything other than "0" and the need for core dumps is not documented with the information system security officer (ISSO) as an operational requirement for all domains that have the "core" item assigned, this is a finding.

Remediation:

Configure the operating system to disable core dumps for all users.
Add the following line to the top of the /etc/security/limits.conf or in a single ".conf" file defined in /etc/security/limits.d/:

```
* hard core 0
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.39 RHEL-09-213100 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must disable acquiring, saving, and processing core dumps.

```
GROUP ID: V-257815
RULE ID: SV-257815r991589
```

Rationale:

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems.

Audit:

Verify RHEL 9 is not configured to acquire, save, or process core dumps with the following command:

```
$ sudo systemctl status systemd-coredump.socket

systemd-coredump.socket
Loaded: masked (Reason: Unit systemd-coredump.socket is masked.)
Active: inactive (dead)
```

If the "systemd-coredump.socket" is loaded and not masked and the need for core dumps is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Configure the system to disable the systemd-coredump.socket with the following command:

```
$ sudo systemctl mask --now systemd-coredump.socket
```

Created symlink /etc/systemd/system/systemd-coredump.socket -> /dev/null
Reload the daemon for this change to take effect.

```
$ sudo systemctl daemon-reload
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.40 RHEL-09-213105 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must disable the use of user namespaces.

```
GROUP ID: V-257816
RULE ID: SV-257816r1014825
```

Rationale:

User namespaces are used primarily for Linux containers. The value "0" disallows the use of user namespaces.

Audit:

Verify RHEL 9 disables the use of user namespaces with the following commands:

```
$ sudo sysctl user.max_user_namespaces

user.max_user_namespaces = 0
```

If the returned line does not have a value of "0", or a line is not returned, this is a finding.
Check that the configuration files are present to enable this kernel parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F user.max_user_namespaces | tail -1
user.max_user_namespaces = 0
```

If the network parameter "user.max_user_namespaces" is not equal to "0", or nothing is returned, this is a finding.
If the use of namespaces is operationally required and documented with the information system security manager (ISSM), this is not a finding.

Remediation:

Configure RHEL 9 to disable the use of user namespaces by adding the following line to a file, in the "/etc/sysctl.d" directory:

```
user.max_user_namespaces = 0
```

The system configuration files need to be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.41 RHEL-09-213110 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must implement nonexecutable data to protect its memory from unauthorized code execution.

```
GROUP ID: V-257817
RULE ID: SV-257817r1069383
```

Rationale:

ExecShield uses the segmentation feature on all x86 systems to prevent execution in memory higher than a certain address. It writes an address as a limit in the code segment descriptor, to control where code can be executed, on a per-process basis. When the kernel places a process's memory regions such as the stack and heap higher than this address, the hardware prevents execution in that address range. This is enabled by default on the latest Red Hat and Fedora systems if supported by the hardware.

Checking dmesg will return a false-positive if the system has generated enough kernel messages that the "(Execute Disable) protection: active" line is no longer present in the output from dmesg(1). A better way to ensure that ExecShield is enabled is to first ensure all processors support the NX feature, and then to check that noexec was not passed to the kernel command line.

Audit:

Verify ExecShield is enabled on 64-bit RHEL 9 systems.
Run the following command:

```
$ grep ^flags /proc/cpuinfo | grep -Ev '([^[:alnum:]])(nx)([^[:alnum:]]|$)'
```

If any output is returned, this is a finding.
Next, run the following command:

```
$ sudo grubby --info=ALL | grep args | grep -E
'([^[:alnum:]])(noexec)([^[:alnum:]])'
```

If any output is returned, this is a finding.

Remediation:

If /proc/cpuinfo shows that one or more processors do not enable ExecShield (lack the "nx" feature flag), verify that the NX/XD feature is not disabled in the BIOS or UEFI. If it is disabled, enable it.
If the noexec option is present on the kernel command line, update the GRUB 2 bootloader configuration to remove it by running the following command:

```
$ sudo grubby --update-kernel=ALL --remove-args=noexec
```

Additional Information:

CCI-002824 Implement organization-defined controls to protect its memory from unauthorized code execution.

- NIST SP 800-53 Revision 4 :: SI-16
- NIST SP 800-53 Revision 5 :: SI-16

1.42 RHEL-09-213115 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The kdump service on RHEL 9 must be disabled.

```
GROUP ID: V-257818
RULE ID: SV-257818r1044876
```

Rationale:

Kernel core dumps may contain the full contents of system memory at the time of the crash. Kernel core dumps 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. Unless the system is used for kernel development or testing, there is little need to run the kdump service.

Audit:

Verify that the kdump service is disabled in system boot configuration with the following command:

```
$ sudo systemctl is-enabled  kdump

disabled
```

Verify that the kdump service is not active (i.e., not running) through current runtime configuration with the following command:

```
$ sudo systemctl is-active kdump

masked
```

Verify that the kdump service is masked with the following command:

```
$ sudo systemctl show  kdump  | grep "LoadState\|UnitFileState"

LoadState=masked
UnitFileState=masked
```

If the "kdump" service is loaded or active, and is not masked, this is a finding.

Remediation:

Disable and mask the kdump service on RHEL 9.
To disable the kdump service run the following command:

```
$ sudo systemctl disable --now kdump
```

To mask the kdump service run the following command:

```
$ sudo systemctl mask --now kdump
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.43 RHEL-09-214010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must ensure cryptographic verification of vendor software packages.

```
GROUP ID: V-257819
RULE ID: SV-257819r1015075
```

Rationale:

Impact:

Cryptographic verification of vendor software packages ensures that all software packages are obtained from a valid source and protects against spoofing that could lead to installation of malware on the system. Red Hat cryptographically signs all software packages, which includes updates, with a GPG key to verify that they are valid.

Audit:

Confirm Red Hat package-signing keys are installed on the system and verify their fingerprints match vendor values.
Note: For RHEL 9 software packages, Red Hat uses GPG keys labeled "release key 2" and "auxiliary key 3". The keys are defined in key file "/etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release" by default.
List Red Hat GPG keys installed on the system:

```
$ sudo rpm -q --queryformat "%{SUMMARY}\n" gpg-pubkey | grep -i "red hat"

Red Hat, Inc. (release key 2) <security@redhat.com> public key
Red Hat, Inc. (auxiliary key 3) <security@redhat.com> public key
```

If Red Hat GPG keys "release key 2" and "auxiliary key 3" are not installed, this is a finding.
List key fingerprints of installed Red Hat GPG keys:

```
$ sudo gpg -q --keyid-format short --with-fingerprint /etc/pki/rpm-gpg/RPM-
GPG-KEY-redhat-release
```

If key file "/etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release" is missing, this is a finding.
Example output:

```
pub   rsa4096/FD431D51 2009-10-22 [SC]
      Key fingerprint = 567E 347A D004 4ADE 55BA  8A5F 199E 2F91 FD43 1D51
uid                   Red Hat, Inc. (release key 2) <security@redhat.com>
pub   rsa4096/5A6340B3 2022-03-09 [SC]
      Key fingerprint = 7E46 2425 8C40 6535 D56D  6F13 5054 E4A4 5A63 40B3
uid                   Red Hat, Inc. (auxiliary key 3) <security@redhat.com>
```

Compare key fingerprints of installed Red Hat GPG keys with fingerprints listed for RHEL 9 on Red Hat "Product Signing Keys" webpage at https://access.redhat.com/security/team/key.
If key fingerprints do not match, this is a finding.

Remediation:

Install Red Hat package-signing keys on the system and verify their fingerprints match vendor values.
Insert RHEL 9 installation disc or attach RHEL 9 installation image to the system. Mount the disc or image to make the contents accessible inside the system.
Assuming the mounted location is "/media/cdrom", use the following command to copy Red Hat GPG key file onto the system:

```
$ sudo cp /media/cdrom/RPM-GPG-KEY-redhat-release /etc/pki/rpm-gpg/
```

Import Red Hat GPG keys from key file into system keyring:

```
$ sudo rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

Using the steps listed in the Check Text, confirm the newly imported keys show as installed on the system and verify their fingerprints match vendor values.

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5 :: CM-14

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.

- NIST SP 800-53 Revision 4 :: CM-5 (3)

1.44 RHEL-09-214015 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

RHEL 9 must check the GPG signature of software packages originating from external software repositories before installation.

```
GROUP ID: V-257820
RULE ID: SV-257820r1044878
```

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.

All software packages must be signed with a cryptographic key recognized and approved by the organization.

Verifying the authenticity of software prior to installation validates the integrity of the software package received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor.

Audit:

Verify that dnf always checks the GPG signature of software packages originating from external software repositories before installation:

```
$ grep -w gpgcheck /etc/dnf/dnf.conf

gpgcheck=1
```

If "gpgcheck" is not set to "1", or if the option is missing or commented out, ask the system administrator how the GPG signatures of software packages are being verified. If there is no process to verify GPG signatures that is approved by the organization, this is a finding.

Remediation:

Configure dnf to always check the GPG signature of software packages originating from external software repositories before installation.
Add or update the following line in the [main] section of the /etc/dnf/dnf.conf file:

```
gpgcheck=1
```

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5 :: CM-14

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.

- NIST SP 800-53 Revision 4 :: CM-5 (3)

1.45 RHEL-09-214020 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

RHEL 9 must check the GPG signature of locally installed software packages before installation.

```
GROUP ID: V-257821
RULE ID: SV-257821r1015077
```

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.

All software packages must be signed with a cryptographic key recognized and approved by the organization.

Verifying the authenticity of software prior to installation validates the integrity of the software package received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor.

Audit:

Verify that dnf always checks the GPG signature of locally installed software packages before installation:

```
$ grep localpkg_gpgcheck /etc/dnf/dnf.conf

localpkg_gpgcheck=1
```

If "localpkg_gpgcheck" is not set to "1", or if the option is missing or commented out, ask the system administrator how the GPG signatures of local software packages are being verified.
If there is no process to verify GPG signatures that is approved by the organization, this is a finding.

Remediation:

Configure dnf to always check the GPG signature of local software packages before installation.
Add or update the following line in the [main] section of the /etc/dnf/dnf.conf file:

```
localpkg_gpgcheck=1
```

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5 :: CM-14

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.

- NIST SP 800-53 Revision 4 :: CM-5 (3)

1.46 RHEL-09-214025 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

RHEL 9 must have GPG signature verification enabled for all software repositories.

```
GROUP ID: V-257822
RULE ID: SV-257822r1044880
```

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.

All software packages must be signed with a cryptographic key recognized and approved by the organization.

Verifying the authenticity of software prior to installation validates the integrity of the software package received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor.

Audit:

Verify that all software repositories defined in "/etc/yum.repos.d/" have been configured with "gpgcheck" enabled:

```
$ grep -w gpgcheck /etc/yum.repos.d/*.repo | more

gpgcheck = 1
```

If "gpgcheck" is not set to "1" for all returned lines, this is a finding.

Remediation:

Configure all software repositories defined in "/etc/yum.repos.d/" to have "gpgcheck" enabled:

```
$ sudo sed -i 's/gpgcheck\s*=.*/gpgcheck=1/g' /etc/yum.repos.d/*
```

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5 :: CM-14

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.

- NIST SP 800-53 Revision 4 :: CM-5 (3)

1.47 RHEL-09-214030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must be configured so that the cryptographic hashes of system files match vendor values.

```
GROUP ID: V-257823
RULE ID: SV-257823r1051231
```

Rationale:

The hashes of important files such as system executables should match the information given by the RPM database. Executables with erroneous hashes could be a sign of nefarious activity on the system.

Audit:

Verify that RHEL 9 is configured so that the cryptographic hashes of system files match vendor values.
List files on the system that have file hashes different from what is expected by the RPM database with the following command:

```
$ sudo rpm -Va --noconfig | awk '$1 ~ /..5/ && $2 != "c"'
```

If there is output, this is a finding.

Remediation:

Configure RHEL 9 so that the cryptographic hashes of system files match vendor values.
Given output from the check command, identify the package that provides the output and reinstall it. The following trimmed example output shows a package that has failed verification, been identified, and been reinstalled:

```
$ sudo rpm -Va --noconfig | awk '$1 ~ /..5/ && $2 != "c"'
S.5....T.    /usr/bin/znew
$ sudo dnf provides /usr/bin/znew
[...]
gzip-1.10-8.el9.x86_64 : The GNU data compression program
[...]
$ sudo dnf -y reinstall gzip
[...]
$ sudo rpm -Va --noconfig | awk '$1 ~ /..5/ && $2 != "c"'
[no output]
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.48 RHEL-09-214035 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

RHEL 9 must remove all software components after updated versions have been installed.

```
GROUP ID: V-257824
RULE ID: SV-257824r1044886
```

Rationale:

Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by some adversaries.

Audit:

Verify RHEL 9 removes all software components after updated versions have been installed with the following command:

```
$ grep -i clean_requirements_on_remove /etc/dnf/dnf.conf

clean_requirements_on_remove=True
```

If "clean_requirements_on_remove" is not set to "True", this is a finding.

Remediation:

Configure RHEL 9 to remove all software components after updated versions have been installed.
Edit the file /etc/dnf/dnf.conf by adding or editing the following line:

```
 clean_requirements_on_remove=True
```

Additional Information:

CCI-002617 Remove previous versions of organization-defined software components after updated versions have been installed.

- NIST SP 800-53 Revision 4 :: SI-2 (6)
- NIST SP 800-53 Revision 5 :: SI-2 (6)

1.49 RHEL-09-215010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 subscription-manager package must be installed.

```
GROUP ID: V-257825
RULE ID: SV-257825r1044888
```

Rationale:

The Red Hat Subscription Manager application manages software subscriptions and software repositories for installed software products on the local system. It communicates with backend servers, such as the Red Hat Customer Portal or an on-premise instance of Subscription Asset Manager, to register the local system and grant access to software resources determined by the subscription entitlement.

Audit:

Verify that RHEL 9 subscription-manager package is installed with the following command:

```
$ dnf list --installed subscription-manager
```

Example output:

```
subscription-manager.x86_64          1.29.26-3.el9_0
```

If the "subscription-manager" package is not installed, this is a finding.

Remediation:

The subscription-manager package can be installed with the following command:

```
$ sudo dnf install subscription-manager
```

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5 :: CM-14

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.

- NIST SP 800-53 Revision 4 :: CM-5 (3)

1.50 RHEL-09-215015 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

RHEL 9 must not have a File Transfer Protocol (FTP) server package installed.

```
GROUP ID: V-257826
RULE ID: SV-257826r1044890
```

Rationale:

The FTP service provides an unencrypted remote access that does not provide for the confidentiality and integrity of user passwords or the remote session. If a privileged user were to log on using this service, the privileged user password could be compromised. SSH or other encrypted file transfer methods must be used in place of this service.

Removing the "vsftpd" package decreases the risk of accidental activation.

Satisfies: SRG-OS-000074-GPOS-00042, SRG-OS-000095-GPOS-00049, SRG-OS-000480-GPOS-00227

Audit:

Verify that RHEL 9 does not have a File Transfer Protocol (FTP) server package installed with the following command:

```
$ rpm -q vsftpd

package vsftpd is not installed
```

If the "ftp" package is installed, this is a finding.

Remediation:

The ftp package can be removed with the following command (using vsftpd as an example):

```
$ sudo dnf remove vsftpd
```

Additional Information:

CCI-000197 For password-based authentication, transmit passwords only cryptographically-protected channels.

- NIST SP 800-53 :: IA-5 (1) (c)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (c)
- NIST SP 800-53 Revision 5 :: IA-5 (1) (c)
- NIST SP 800-53A :: IA-5 (1).1 (v)

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.51 RHEL-09-215020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not have the sendmail package installed.

```
GROUP ID: V-257827
RULE ID: SV-257827r1044892
```

Rationale:

The sendmail software was not developed with security in mind, and its design prevents it from being effectively contained by SELinux. Postfix must be used instead.

Satisfies: SRG-OS-000480-GPOS-00227, SRG-OS-000095-GPOS-00049

Audit:

Verify that the sendmail package is not installed with the following command:

```
$ dnf list --installed sendmail

Error: No matching Packages to list
```

If the "sendmail" package is installed, this is a finding.

Remediation:

Remove the sendmail package with the following command:

```
$ sudo dnf remove sendmail
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.52 RHEL-09-215025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not have the nfs-utils package installed.

```
GROUP ID: V-257828
RULE ID: SV-257828r1044894
```

Rationale:

"nfs-utils" provides a daemon for the kernel NFS server and related tools. This package also contains the "showmount" program. "showmount" queries the mount daemon on a remote host for information about the Network File System (NFS) server on the remote host. For example, "showmount" can display the clients that are mounted on that host.

Audit:

Verify that the nfs-utils package is not installed with the following command:

```
$ dnf list --installed nfs-utils

Error: No matching Packages to list
```

If the "nfs-utils" package is installed, this is a finding.

Remediation:

Remove the nfs-utils package with the following command:

```
$ sudo dnf remove nfs-utils
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.53 RHEL-09-215030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not have the ypserv package installed.

```
GROUP ID: V-257829
RULE ID: SV-257829r1044896
```

Rationale:

The NIS service provides an unencrypted authentication service, which does not provide for the confidentiality and integrity of user passwords or the remote session.

Removing the "ypserv" package decreases the risk of the accidental (or intentional) activation of NIS or NIS+ services.

Audit:

Verify that the ypserv package is not installed with the following command:

```
$ dnf list --installed ypserv

Error: No matching Packages to list
```

If the "ypserv" package is installed, this is a finding.

Remediation:

Remove the ypserv package with the following command:

```
$ sudo dnf remove ypserv
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.54 RHEL-09-215035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not have the rsh-server package installed.

```
GROUP ID: V-257830
RULE ID: SV-257830r958478
```

Rationale:

The "rsh-server" service provides unencrypted remote access service, which 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 login using this service, the privileged user password could be compromised. The "rsh-server" package provides several obsolete and insecure network services. Removing it decreases the risk of accidental (or intentional) activation of those services.

Audit:

Verify that the rsh-server package is not installed with the following command:

```
$ sudo dnf list --installed rsh-server
```

Error: No matching Packages to list
If the "rsh-server" package is installed, this is a finding.

Remediation:

Remove the rsh-server package with the following command:

```
$ sudo dnf remove rsh-server
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.55 RHEL-09-215040 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not have the telnet-server package installed.

```
GROUP ID: V-257831
RULE ID: SV-257831r1044898
```

Rationale:

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

The telnet service provides an unencrypted remote access service, which does not provide for the confidentiality and integrity of user passwords or the remote session. If a privileged user were to login using this service, the privileged user password could be compromised.

Removing the "telnet-server" package decreases the risk of accidental (or intentional) activation of the telnet service.

Audit:

Verify that the telnet-server package is not installed with the following command:

```
$ dnf list --installed telnet-server

Error: No matching Packages to list
```

If the "telnet-server" package is installed, this is a finding.

Remediation:

Remove the telnet-server package with the following command:

```
$ sudo dnf remove telnet-server
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.56 RHEL-09-215045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not have the gssproxy package installed.

```
GROUP ID: V-257832
RULE ID: SV-257832r1044900
```

Rationale:

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

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations (e.g., key missions, functions).

The gssproxy package is a proxy for GSS API credential handling and could expose secrets on some networks. It is not needed for normal function of the OS.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000480-GPOS-00227

Audit:

Verify that the gssproxy package is not installed with the following command:

```
$ dnf list --installed gssproxy

Error: No matching Packages to list
```

If the "gssproxy" package is installed and is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Remove the gssproxy package with the following command:

```
$ sudo dnf remove gssproxy
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.57 RHEL-09-215050 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not have the iprutils package installed.

```
GROUP ID: V-257833
RULE ID: SV-257833r1044902
```

Rationale:

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

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

The iprutils package provides a suite of utilities to manage and configure SCSI devices supported by the ipr SCSI storage device driver.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000480-GPOS-00227

Audit:

Verify that the iprutils package is not installed with the following command:

```
$ dnf list --installed iprutils

Error: No matching Packages to list
```

If the "iprutils" package is installed and is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Remove the iprutils package with the following command:

```
$ sudo dnf remove iprutils
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.58 RHEL-09-215055 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not have the tuned package installed.

```
GROUP ID: V-257834
RULE ID: SV-257834r1044904
```

Rationale:

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

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

The tuned package contains a daemon that tunes the system settings dynamically. It does so by monitoring the usage of several system components periodically. Based on that information, components will then be put into lower or higher power savings modes to adapt to the current usage. The tuned package is not needed for normal OS operations.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000480-GPOS-00227

Audit:

Verify that the tuned package is not installed with the following command:

```
$ dnf list --installed tuned

Error: No matching Packages to list
```

If the "tuned" package is installed and is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Remove the tuned package with the following command:

```
$ sudo dnf remove tuned
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.59 RHEL-09-215060 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

RHEL 9 must not have a Trivial File Transfer Protocol (TFTP) server package installed.

```
GROUP ID: V-257835
RULE ID: SV-257835r1069368
```

Rationale:

Removing the "tftp-server" package decreases the risk of the accidental (or intentional) activation of tftp services.

If TFTP is required for operational support (such as transmission of router configurations), its use must be documented with the information systems security manager (ISSM), restricted to only authorized personnel, and have access control rules established.

Audit:

Verify that RHEL 9 does not have a "tftp-server" package installed with the following command:

```
$ dnf list --installed tftp-server

Error: No matching Packages to list
```

If the "tftp-server" package is installed, this is a finding.

Remediation:

The "tftp-server" package can be removed with the following command:

```
$ sudo dnf remove tftp-server
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.60 RHEL-09-215065 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not have the quagga package installed.

```
GROUP ID: V-257836
RULE ID: SV-257836r1044908
```

Rationale:

Quagga is a network routing software suite providing implementations of Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Border Gateway Protocol (BGP) for Unix and Linux platforms.

If there is no need to make the router software available, removing it provides a safeguard against its activation.

Audit:

Verify that the quagga package is not installed with the following command:

```
$ dnf list --installed quagga

Error: No matching Packages to list
```

If the "quagga" package is installed and is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Remove the quagga package with the following command:

```
$ sudo dnf remove quagga
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.61 RHEL-09-215070 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

A graphical display manager must not be installed on RHEL 9 unless approved.

```
GROUP ID: V-257837
RULE ID: SV-257837r1044910
```

Rationale:

Unnecessary service packages must not be installed to decrease the attack surface of the system. Graphical display managers have a long history of security vulnerabilities and must not be used, unless approved and documented.

Audit:

Verify that a graphical user interface is not installed with the following command:

```
$ dnf list --installed "xorg-x11-server-common"
Error: No matching Packages to list
```

If the "xorg-x11-server-common" package is installed, and the use of a graphical user interface has not been documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Document the requirement for a graphical user interface with the ISSO or remove all xorg packages with the following command:
Warning: If you are accessing the system through the graphical user interface, change to the multi-user.target with the following command:

```
$ sudo systemctl isolate multi-user.target
```

Warning: Removal of the graphical user interface will immediately render it useless. The following commands must not be run from a virtual terminal emulator in the graphical interface.

```
$ sudo dnf remove "xorg*"
$ sudo systemctl set-default multi-user.target
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.62 RHEL-09-215075 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must have the openssl-pkcs11 package installed.

```
GROUP ID: V-257838
RULE ID: SV-257838r1044912
```

Rationale:

Without the use of multifactor authentication, the ease of access to privileged functions is greatly increased. Multifactor authentication requires using two or more factors to achieve authentication. A privileged account is defined as an information system account with authorizations of a privileged user. The DOD common access card (CAC) with DOD-approved PKI is an example of multifactor authentication.

Satisfies: SRG-OS-000105-GPOS-00052, SRG-OS-000375-GPOS-00160, SRG-OS-000376-GPOS-00161, SRG-OS-000377-GPOS-00162

Audit:

Note: If the system administrator demonstrates the use of an approved alternate multifactor authentication method, this requirement is Not Applicable.
Verify that RHEL 9 has the openssl-pkcs11 package installed with the following command:

```
$ dnf list --installed openssl-pkcs11
```

Example output:

```
openssl-pkcs.i686          0.4.11-7.el9
openssl-pkcs.x86_64          0.4.11-7.el9
```

If the "openssl-pkcs11" package is not installed, this is a finding.

Remediation:

The openssl-pkcs11 package can be installed with the following command:

```
$ sudo dnf install openssl-pkcs11
```

Additional Information:

CCI-000765 Implement multifactor authentication for network access to privileged accounts.

- NIST SP 800-53 :: IA-2 (1)
- NIST SP 800-53 Revision 4 :: IA-2 (1)
- NIST SP 800-53 Revision 5 :: IA-2 (1)
- NIST SP 800-53A :: IA-2 (1).1

CCI-004046 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 5 :: IA-2 (6) (a)

CCI-001953 Accepts Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4 :: IA-2 (12)
- NIST SP 800-53 Revision 5 :: IA-2 (12)

CCI-001954 Electronically verifies Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4 :: IA-2 (12)
- NIST SP 800-53 Revision 5 :: IA-2 (12)

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.

- NIST SP 800-53 Revision 4 :: IA-2 (11)

1.63 RHEL-09-215080 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must have the gnutls-utils package installed.

```
GROUP ID: V-257839
RULE ID: SV-257839r991589
```

Rationale:

GnuTLS is a secure communications library implementing the SSL, TLS and DTLS protocols and technologies around them. It provides a simple C language application programming interface (API) to access the secure communications protocols as well as APIs to parse and write X.509, PKCS #12, OpenPGP and other required structures. This package contains command line TLS client and server and certificate manipulation tools.

Audit:

Verify that RHEL 9 has the gnutls-utils package installed with the following command:

```
$ dnf list --installed gnutls-utils
```

Example output:

```
gnutls-utils.x86_64          3.7.3-9.el9
```

If the "gnutls-utils" package is not installed, this is a finding.

Remediation:

The gnutls-utils package can be installed with the following command:

```
$ sudo dnf install gnutls-utils
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.64 RHEL-09-215085 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must have the nss-tools package installed.

```
GROUP ID: V-257840
RULE ID: SV-257840r991589
```

Rationale:

Network Security Services (NSS) is a set of libraries designed to support cross-platform development of security-enabled client and server applications. Install the "nss-tools" package to install command-line tools to manipulate the NSS certificate and key database.

Audit:

Verify that RHEL 9 has the nss-tools package installed with the following command:

```
$ dnf list --installed nss-tools
```

Example output:

```
nss-tools.x86_64          3.71.0-7.el9
```

If the "nss-tools" package is not installed, this is a finding.

Remediation:

The nss-tools package can be installed with the following command:

```
$ sudo dnf install nss-tools
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.65 RHEL-09-215090 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must have the rng-tools package installed.

```
GROUP ID: V-257841
RULE ID: SV-257841r1044914
```

Rationale:

"rng-tools" provides hardware random number generator tools, such as those used in the formation of x509/PKI certificates.

Audit:

Verify that RHEL 9 has the rng-tools package installed with the following command:

```
$ dnf list --installed rng-tools
```

Example output:

```
rng-tools.x86_64          6.14-2.git.b2b7934e.el9
```

If the "rng-tools" package is not installed, this is a finding.

Remediation:

The rng-tools package can be installed with the following command:

```
$ sudo dnf install rng-tools
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.66 RHEL-09-215095 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must have the s-nail package installed.

```
GROUP ID: V-257842
RULE ID: SV-257842r1044916
```

Rationale:

The "s-nail" package provides the mail command required to allow sending email notifications of unauthorized configuration changes to designated personnel.

Audit:

Verify that RHEL 9 is configured to allow sending email notifications.
Note: The "s-nail" package provides the "mail" command that is used to send email messages.
Verify that the "s-nail" package is installed on the system:

```
$ dnf list --installed s-nail

s-nail.x86_64          14.9.22-6.el9
```

If "s-nail" package is not installed, this is a finding.

Remediation:

The s-nail package can be installed with the following command:

```
$ sudo dnf install s-nail
```

Additional Information:

CCI-001744 Implement organization-defined security responses automatically if baseline configurations are changed in an unauthorized manner.

- NIST SP 800-53 Revision 4 :: CM-3 (5)
- NIST SP 800-53 Revision 5 :: CM-3 (5)

1.67 RHEL-09-215100 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must have the crypto-policies package installed.

```
GROUP ID: V-258234
RULE ID: SV-258234r1051250
```

Rationale:

Centralized cryptographic policies simplify applying secure ciphers across an operating system and the applications that run on that operating system. Use of weak or untested encryption algorithms undermines the purposes of using encryption to protect data.

Satisfies: SRG-OS-000396-GPOS-00176, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174

Audit:

Verify that the RHEL 9 crypto-policies package is installed with the following command:

```
$ dnf list --installed crypto-policies
```

Example output:

```
crypto-policies.noarch          20240828-2.git626aa59.el9_5
```

If the crypto-policies package is not installed, this is a finding.

Remediation:

Install the crypto-policies package (if the package is not already installed) with the following command:

```
$ sudo dnf -y install crypto-policies
```

Additional Information:

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4 :: SC-13
- NIST SP 800-53 Revision 5 :: SC-13 b

CCI-002890 Implement organization-defined cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4 :: MA-4 (6)
- NIST SP 800-53 Revision 5 :: MA-4 (6)

CCI-003123 Implement organization-defined cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4 :: MA-4 (6)
- NIST SP 800-53 Revision 5 :: MA-4 (6)

1.68 RHEL-09-215101 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must have the Postfix package installed.

```
GROUP ID: V-272488
RULE ID: SV-272488r1082178
```

Rationale:

Postfix is a free, open-source mail transfer agent (MTA) that sends and receives emails. It is a server-side application that can be used to set up a local mail server, create a null-client mail relay, use a Postfix server as a destination for multiple domains, or choose an LDAP directory instead of files for lookups. Postfix supports protocols such as LDAP, SMTP AUTH (SASL), and TLS. It uses the Simple Mail Transfer Protocol (SMTP) to transfer emails between servers.

Satisfies: SRG-OS-000304-GPOS-00121, SRG-OS-000343-GPOS-00134, SRG-OS-000363-GPOS-00150, SRG-OS-000447-GPOS-00201

Audit:

Verify that RHEL 9 has the Postfix package installed with the following command:

```
$ sudo dnf list --installed postfix
```

Example output:

```
postfix.x86_64                              2:3.5.25-1.el9
```

If the "postfix" package is not installed, this is a finding.

Remediation:

Install the Postfix package with the following command:

```
$ sudo dnf install postfix
```

Additional Information:

CCI-000015 Support the management of system accounts using (organization-defined automated mechanisms).

- NIST SP 800-53 :: AC-2 (1)
- NIST SP 800-53 Revision 4 :: AC-2 (1)
- NIST SP 800-53 Revision 5 :: AC-2 (1)
- NIST SP 800-53A :: AC-2 (1).1

1.69 RHEL-09-215105 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must implement a FIPS 140-3 compliant systemwide cryptographic policy.

```
GROUP ID: V-258241
RULE ID: SV-258241r1051259
```

Rationale:

Centralized cryptographic policies simplify applying secure ciphers across an operating system and the applications that run on that operating system. Use of weak or untested encryption algorithms undermines the purposes of using encryption to protect data.

Satisfies: SRG-OS-000396-GPOS-00176, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174

Audit:

Verify that RHEL 9 is set to use a FIPS 140-3 compliant systemwide cryptographic policy.

```
$ update-crypto-policies --show

FIPS
```

If the systemwide crypto policy is not set to "FIPS", this is a finding.
Inspect the contents of the REQUIRE.pmod file (if it exists) to ensure that only authorized modifications to the current policy are included with the following command:

```
$ cat /etc/crypto-policies/policies/modules/REQUIRE.pmod
```

Note: If subpolicies have been configured, they could be listed in a colon-separated list starting with FIPS as follows FIPS:<SUBPOLICY-NAME>:<SUBPOLICY-NAME>. This is not a finding.
If the AD-SUPPORT subpolicy module is included (e.g., "FIPS:AD-SUPPORT"), and Active Directory support is not documented as an operational requirement with the information system security officer (ISSO), this is a finding.
If the NO-ENFORCE-EMS subpolicy module is included (e.g., "FIPS:NO-ENFORCE-EMS"), and not enforcing EMS is not documented as an operational requirement with the ISSO, this is a finding.
Verify the current minimum crypto-policy configuration with the following commands:

```
$ grep -E 'rsa_size|hash' /etc/crypto-policies/state/CURRENT.pol
hash = SHA2-256 SHA2-384 SHA2-512 SHA2-224 SHA3-256 SHA3-384 SHA3-512 SHAKE-
256
min_rsa_size = 2048
```

If the "hash" values do not include at least the following FIPS 140-3 compliant algorithms "SHA2-256 SHA2-384 SHA2-512 SHA2-224 SHA3-256 SHA3-384 SHA3-512 SHAKE-256", this is a finding.
If there are algorithms that include "SHA1" or a hash value less than "256" this is a finding.
If the "min_rsa_size" is not set to a value of at least 2048, this is a finding.
If these commands do not return any output, this is a finding.

Remediation:

Configure RHEL 9 to use a FIPS 140-3 compliant systemwide cryptographic policy.
Create subpolicies for enhancements to the systemwide crypto-policy with the following commands:
Create or edit the SCOPES-AND-WILDCARDS policy module in a text editor and insert options that modify the systemwide cryptographic policy as follows:

```
$ sudo vi /etc/crypto-policies/policies/modules/SCOPES-AND-WILDCARDS.pmod
```

Add the following lines to the policy:

```
# Disable CHACHA20-POLY1305 for the TLS protocol (OpenSSL, GnuTLS, NSS, and
OpenJDK)
cipher@TLS = -CHACHA20-POLY1305

# Disable all CBC mode ciphers for the SSH protocol (libssh and OpenSSH)
cipher@SSH = -*-CBC
```

Create or edit the OPENSSH-SUBPOLICY module in a text editor and insert options that modify the systemwide crypto-policy as follows:

```
$ sudo vi /etc/crypto-policies/policies/modules/OPENSSH-SUBPOLICY.pmod
```

Add the following lines to the policy:

```
# Define ciphers for OpenSSH
cipher@SSH=AES-256-GCM AES-128-GCM AES-256-CTR AES-128-CTR

# Define MACs for OpenSSH
mac@SSH=HMAC-SHA2-512 HMAC-SHA2-256
```

Create or edit the REQUIRE.pmod file and add the following lines to include the subpolicies in the FIPS configuration with the following command:

```
$ sudo vi /etc/crypto-policies/policies/modules/REQUIRE.pmod
```

Add the following lines to REQUIRE.pmod:

```
@OPENSSH-SUBPOLICY
@SCOPES-AND-WILDCARDS
```

Apply the policy enhancements to the FIPS systemwide cryptographic policy level with the following command:

```
$ sudo update-crypto-policies --set FIPS
```

Note: If additional subpolicies are being employed, they should be added to the REQUIRE.pmod as well. REQUIRE.pmod is included in the systemwide crypto-policy when it is set.
To make the cryptographic settings effective for already running services and applications, restart the system:

```
$ sudo reboot
```

Additional Information:

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4 :: SC-13
- NIST SP 800-53 Revision 5 :: SC-13 b

CCI-002890 Implement organization-defined cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4 :: MA-4 (6)
- NIST SP 800-53 Revision 5 :: MA-4 (6)

CCI-003123 Implement organization-defined cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4 :: MA-4 (6)
- NIST SP 800-53 Revision 5 :: MA-4 (6)

1.70 RHEL-09-231010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

A separate RHEL 9 file system must be used for user home directories (such as /home or an equivalent).

```
GROUP ID: V-257843
RULE ID: SV-257843r991589
```

Rationale:

Ensuring that "/home" is mounted on its own partition enables the setting of more restrictive mount options, and also helps ensure that users cannot trivially fill partitions used for log or audit data storage.

Audit:

Verify that a separate file system/partition has been created for "/home" with the following command:

```
$ mount | grep /home

UUID=fba5000f-2ffa-4417-90eb-8c54ae74a32f on /home type ext4
(rw,nodev,nosuid,noexec,seclabel)
```

If a separate entry for "/home" is not in use, this is a finding.

Remediation:

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

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.71 RHEL-09-231015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must use a separate file system for /tmp.

```
GROUP ID: V-257844
RULE ID: SV-257844r1044918
```

Rationale:

The "/tmp" partition is used as temporary storage by many programs. Placing "/tmp" in its own partition enables the setting of more restrictive mount options, which can help protect programs that use it.

Audit:

Verify that a separate file system/partition has been created for "/tmp" with the following command:

```
$ mount | grep /tmp

/dev/mapper/rhel-tmp on /tmp type xfs (rw,nodev,nosuid,noexec,seclabel)
```

If a separate entry for "/tmp" is not in use, this is a finding.

Remediation:

Migrate the "/tmp" path onto a separate file system.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.72 RHEL-09-231020 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

RHEL 9 must use a separate file system for /var.

```
GROUP ID: V-257845
RULE ID: SV-257845r1044920
```

Rationale:

Ensuring that "/var" is mounted on its own partition enables the setting of more restrictive mount options. This helps protect system services such as daemons or other programs which use it. It is not uncommon for the "/var" directory to contain world-writable directories installed by other software packages.

Audit:

Verify that a separate file system/partition has been created for "/var" with the following command:

```
$ mount | grep /var

/dev/mapper/rootvg-varlv on /var type xfs
(rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota)
```

Note: Options displayed for mount may differ.
If a separate entry for "/var" is not in use, this is a finding.

Remediation:

Migrate the "/var" path onto a separate file system.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.73 RHEL-09-231025 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

RHEL 9 must use a separate file system for /var/log.

```
GROUP ID: V-257846
RULE ID: SV-257846r1044922
```

Rationale:

Placing "/var/log" in its own partition enables better separation between log files and other files in "/var/".

Audit:

Verify that a separate file system/partition has been created for "/var/log" with the following command:

```
$ mount | grep /var/log

/dev/mapper/rhel-var_log on /var/log type xfs
(rw,nosuid,nodev,noexec,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32
k)
```

Note: Options displayed for mount may differ.
If a separate entry for "/var/log" is not in use, this is a finding.

Remediation:

Migrate the "/var/log" path onto a separate file system.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.74 RHEL-09-231030 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

RHEL 9 must use a separate file system for the system audit data path.

Rationale:

Placing "/var/log/audit" in its own partition enables better separation between audit files and other system files, and helps ensure that auditing cannot be halted due to the partition running out of space.

Satisfies: SRG-OS-000341-GPOS-00132, SRG-OS-000480-GPOS-00227

Audit:

Verify that a separate file system/partition has been created for the system audit data path with the following command:
Note: /var/log/audit is used as the example as it is a common location.

```
$ mount | grep /var/log/audit

/dev/mapper/rootvg-varlogaudit on /var/log/audit type xfs
(rw,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota)
```

Note: Options displayed for mount may differ.
If no line is returned, this is a finding.

Remediation:

Migrate the system audit data path onto a separate file system.

Additional Information:

CCI-001849 Allocate audit log storage capacity to accommodate organization-defined audit record retention requirements.

- NIST SP 800-53 Revision 4 :: AU-4
- NIST SP 800-53 Revision 5 :: AU-4

1.75 RHEL-09-231035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must use a separate file system for /var/tmp.

```
GROUP ID: V-257848
RULE ID: SV-257848r1044926
```

Rationale:

The "/var/tmp" partition is used as temporary storage by many programs. Placing "/var/tmp" in its own partition enables the setting of more restrictive mount options, which can help protect programs that use it.

Audit:

Verify that a separate file system/partition has been created for "/var/tmp" with the following command:

```
$ mount | grep /var/tmp

/dev/mapper/rhel-tmp on /var/tmp type xfs
(rw,nosuid,nodev,noexec,relatime,seclabel,attr2,inode64,logbufs=8,logbsize=32
k)
```

Note: Options displayed for mount may differ.
If a separate entry for "/var/tmp" is not in use, this is a finding.

Remediation:

Migrate the "/var/tmp" path onto a separate file system.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.76 RHEL-09-231040 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 file system automount function must be disabled unless required.

```
GROUP ID: V-257849
RULE ID: SV-257849r1044928
```

Rationale:

An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message.

Satisfies: SRG-OS-000114-GPOS-00059, SRG-OS-000378-GPOS-00163, SRG-OS-000480-GPOS-00227

Audit:

Note: If the autofs service is not installed, this requirement is Not Applicable.
Verify that the RHEL 9 file system automount function has been disabled with the following command:

```
$ systemctl is-enabled  autofs

masked
```

If the returned value is not "masked", "disabled", or "Failed to get unit file state for autofs.service for autofs" and is not documented as an operational requirement with the information system security officer (ISSO), this is a finding.

Remediation:

Configure RHEL 9 to disable the ability to automount devices.
The autofs service can be disabled with the following command:

```
$ sudo systemctl mask --now autofs.service
```

Additional Information:

CCI-000778 Uniquely identify organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 :: IA-3
- NIST SP 800-53 Revision 4 :: IA-3
- NIST SP 800-53 Revision 5 :: IA-3
- NIST SP 800-53A :: IA-3.1 (ii)

CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4 :: IA-3
- NIST SP 800-53 Revision 5 :: IA-3

1.77 RHEL-09-231045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent device files from being interpreted on file systems that contain user home directories.

```
GROUP ID: V-257850
RULE ID: SV-257850r1044930
```

Rationale:

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for nonprivileged users to attain unauthorized administrative access.

The only legitimate location for device files is the "/dev" directory located on the root partition, with the exception of chroot jails if implemented.

Audit:

Verify "/home" is mounted with the "nodev" option 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 automatically a finding, as the "nodev" option cannot be used on the "/" system.

```
$ mount | grep /home

tmpfs on /home type xfs (rw,nodev,nosuid,noexec,seclabel)
```

If the "/home" file system is mounted without the "nodev" option, this is a finding.

Remediation:

Modify "/etc/fstab" to use the "nodev" option on the "/home" directory.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.78 RHEL-09-231050 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent files with the setuid and setgid bit set from being executed on file systems that contain user home directories.

```
GROUP ID: V-257851
RULE ID: SV-257851r1044932
```

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 "setguid" files. Executing files from untrusted file systems increases the opportunity for nonprivileged users to attain unauthorized administrative access.

Satisfies: SRG-OS-000368-GPOS-00154, SRG-OS-000480-GPOS-00227

Audit:

Verify "/home" is mounted with the "nosuid" option 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 automatically a finding, as the "nosuid" option cannot be used on the "/" system.

```
$ mount | grep /home

tmpfs on /home type xfs (rw,nodev,nosuid,noexec,seclabel)
```

If the "/home" file system is mounted without the "nosuid" option, this is a finding.

Remediation:

Modify "/etc/fstab" to use the "nosuid" option on the "/home" directory.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.79 RHEL-09-231055 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent code from being executed on file systems that contain user home directories.

```
GROUP ID: V-257852
RULE ID: SV-257852r991589
```

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 nonprivileged users to attain unauthorized administrative access.

Audit:

Verify "/home" is mounted with the "noexec" option 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 automatically a finding, as the "noexec" option cannot be used on the "/" system.

```
$ mount | grep /home

tmpfs on /home type xfs (rw,nodev,nosuid,noexec,seclabel)
```

If the "/home" file system is mounted without the "noexec" option, this is a finding.

Remediation:

Modify "/etc/fstab" to use the "noexec" option on the "/home" directory.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.80 RHEL-09-231065 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent special devices on file systems that are imported via Network File System (NFS).

```
GROUP ID: V-257854
RULE ID: SV-257854r1044934
```

Rationale:

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for nonprivileged users to attain unauthorized administrative access.

Audit:

Note: If no NFS mounts are configured, this requirement is Not Applicable.
Verify RHEL 9 has the "nodev" option configured for all NFS mounts with the following command:

```
$ grep nfs /etc/fstab

192.168.22.2:/mnt/export /data nfs4
rw,nosuid,nodev,noexec,sync,soft,sec=krb5:krb5i:krb5p
```

If the system is mounting file systems via NFS and the "nodev" option is missing, this is a finding.

Remediation:

Update each NFS mounted file system to use the "nodev" option on file systems that are being imported via NFS.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.81 RHEL-09-231070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent code from being executed on file systems that are imported via Network File System (NFS).

```
GROUP ID: V-257855
RULE ID: SV-257855r1044936
```

Rationale:

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

Audit:

Note: If no NFS mounts are configured, this requirement is Not Applicable.
Verify RHEL 9 has the "noexec" option configured for all NFS mounts with the following command:

```
$ grep nfs /etc/fstab

192.168.22.2:/mnt/export /data nfs4
rw,nosuid,nodev,noexec,sync,soft,sec=krb5:krb5i:krb5p
```

If the system is mounting file systems via NFS and the "noexec" option is missing, this is a finding.

Remediation:

Update each NFS mounted file system to use the "noexec" option on file systems that are being imported via NFS.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.82 RHEL-09-231075 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent files with the setuid and setgid bit set from being executed on file systems that are imported via Network File System (NFS).

```
GROUP ID: V-257856
RULE ID: SV-257856r1044938
```

Rationale:

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

Audit:

Note: If no NFS mounts are configured, this requirement is Not Applicable.
Verify RHEL 9 has the "nosuid" option configured for all NFS mounts with the following command:

```
$ grep nfs /etc/fstab

192.168.22.2:/mnt/export /data nfs4
rw,nosuid,nodev,noexec,sync,soft,sec=krb5:krb5i:krb5p
```

If the system is mounting file systems via NFS and the "nosuid" option is missing, this is a finding.

Remediation:

Update each NFS mounted file system to use the "nosuid" option on file systems that are being imported via NFS.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.83 RHEL-09-231080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent code from being executed on file systems that are used with removable media.

```
GROUP ID: V-257857
RULE ID: SV-257857r991589
```

Rationale:

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

Audit:

Verify file systems that are used for removable media are mounted with the "noexec" option with the following command:

```
$ more /etc/fstab

UUID=2bc871e4-e2a3-4f29-9ece-3be60c835222 /mnt/usbflash vfat
noauto,owner,ro,nosuid,nodev,noexec 0 0
```

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

Remediation:

Configure the "/etc/fstab" to use the "noexec" option on file systems that are associated with removable media.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.84 RHEL-09-231085 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent special devices on file systems that are used with removable media.

```
GROUP ID: V-257858
RULE ID: SV-257858r991589
```

Rationale:

The "nodev" mount option causes the system not to interpret character or block special devices. Executing character or blocking special devices from untrusted file systems increases the opportunity for nonprivileged users to attain unauthorized administrative access.

Audit:

Verify file systems that are used for removable media are mounted with the "nodev" option with the following command:

```
$ more /etc/fstab

UUID=2bc871e4-e2a3-4f29-9ece-3be60c835222 /mnt/usbflash vfat
noauto,owner,ro,nosuid,nodev,noexec 0 0
```

If a file system found in "/etc/fstab" refers to removable media and it does not have the "nodev" option set, this is a finding.

Remediation:

Configure the "/etc/fstab" to use the "nodev" option on file systems that are associated with removable media.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.85 RHEL-09-231090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent files with the setuid and setgid bit set from being executed on file systems that are used with removable media.

```
GROUP ID: V-257859
RULE ID: SV-257859r991589
```

Rationale:

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

Audit:

Verify file systems that are used for removable media are mounted with the "nosuid" option with the following command:

```
$ more /etc/fstab

UUID=2bc871e4-e2a3-4f29-9ece-3be60c835222 /mnt/usbflash vfat
noauto,owner,ro,nosuid,nodev,noexec 0 0
```

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

Remediation:

Configure the "/etc/fstab" to use the "nosuid" option on file systems that are associated with removable media.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.86 RHEL-09-231095 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must mount /boot with the nodev option.

```
GROUP ID: V-257860
RULE ID: SV-257860r1044940
```

Rationale:

The only legitimate location for device files is the "/dev" directory located on the root partition. The only exception to this is chroot jails.

Audit:

Verify that the "/boot" mount point has the "nodev" option with the following command:

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

/dev/sda1 on /boot type xfs (rw,nodev,relatime,seclabel,attr2)
```

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

Remediation:

Modify "/etc/fstab" to use the "nodev" option on the "/boot" directory.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.87 RHEL-09-231100 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent files with the setuid and setgid bit set from being executed on the /boot directory.

```
GROUP ID: V-257861
RULE ID: SV-257861r1044941
```

Rationale:

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

Satisfies: SRG-OS-000368-GPOS-00154, SRG-OS-000480-GPOS-00227

Audit:

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

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

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

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

Remediation:

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

Additional Information:

Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.88 RHEL-09-231105 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent files with the setuid and setgid bit set from being executed on the /boot/efi directory.

```
GROUP ID: V-257862
RULE ID: SV-257862r1051265
```

Rationale:

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

Satisfies: SRG-OS-000368-GPOS-00154, SRG-OS-000480-GPOS-00227

Audit:

Note: For systems that use BIOS, this requirement is Not Applicable.
Verify the /boot/efi directory is mounted with the "nosuid" option with the following command:

```
$ mount | grep '\s/boot/efi\s'

/dev/sda1 on /boot/efi type vfat
(rw,nosuid,relatime,fmask=0077,dmask=0077,codepage=437,iocharset=ascii,shortn
ame=winnt,errors=remount-ro)
```

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

Remediation:

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

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.89 RHEL-09-231110 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must mount /dev/shm with the nodev option.

```
GROUP ID: V-257863
RULE ID: SV-257863r958804
```

Rationale:

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for nonprivileged users to attain unauthorized administrative access.

The only legitimate location for device files is the "/dev" directory located on the root partition, with the exception of chroot jails if implemented.

Audit:

Verify "/dev/shm" is mounted with the "nodev" option with the following command:

```
$ mount | grep /dev/shm

tmpfs on /dev/shm type tmpfs (rw,nodev,nosuid,noexec,seclabel)
```

If the /dev/shm file system is mounted without the "nodev" option, this is a finding.

Remediation:

Modify "/etc/fstab" to use the "nodev" option on the "/dev/shm" file system.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.90 RHEL-09-231115 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must mount /dev/shm with the noexec option.

```
GROUP ID: V-257864
RULE ID: SV-257864r958804
```

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 nonprivileged users to attain unauthorized administrative access.

Audit:

Verify "/dev/shm" is mounted with the "noexec" option with the following command:

```
$ mount | grep /dev/shm

tmpfs on /dev/shm type tmpfs (rw,nodev,nosuid,noexec,seclabel)
```

If the /dev/shm file system is mounted without the "noexec" option, this is a finding.

Remediation:

Modify "/etc/fstab" to use the "noexec" option on the "/dev/shm" file system.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.91 RHEL-09-231120 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must mount /dev/shm with the nosuid option.

```
GROUP ID: V-257865
RULE ID: SV-257865r1044946
```

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 "setguid" files. Executing files from untrusted file systems increases the opportunity for nonprivileged users to attain unauthorized administrative access.

Audit:

Verify "/dev/shm" is mounted with the "nosuid" option with the following command:

```
$ mount | grep /dev/shm

tmpfs on /dev/shm type tmpfs (rw,nodev,nosuid,noexec,seclabel)
```

If the /dev/shm file system is mounted without the "nosuid" option, this is a finding.

Remediation:

Modify "/etc/fstab" to use the "nosuid" option on the "/dev/shm" file system.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.92 RHEL-09-231125 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must mount /tmp with the nodev option.

```
GROUP ID: V-257866
RULE ID: SV-257866r958804
```

Rationale:

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for nonprivileged users to attain unauthorized administrative access.

The only legitimate location for device files is the "/dev" directory located on the root partition, with the exception of chroot jails if implemented.

Audit:

Verify "/tmp" is mounted with the "nodev" option:

```
$ mount | grep /tmp

/dev/mapper/rhel-tmp on /tmp type xfs (rw,nodev,nosuid,noexec,seclabel)
```

If the "/tmp" file system is mounted without the "nodev" option, this is a finding.

Remediation:

Modify "/etc/fstab" to use the "nodev" option on the "/tmp" directory.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.93 RHEL-09-231130 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must mount /tmp with the noexec option.

```
GROUP ID: V-257867
RULE ID: SV-257867r958804
```

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 nonprivileged users to attain unauthorized administrative access.

Audit:

Verify "/tmp" is mounted with the "noexec" option:

```
$ mount | grep /tmp

/dev/mapper/rhel-tmp on /tmp type xfs (rw,nodev,nosuid,noexec,seclabel)
```

If the "/tmp" file system is mounted without the "noexec" option, this is a finding.

Remediation:

Modify "/etc/fstab" to use the "noexec" option on the "/tmp" directory.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.94 RHEL-09-231135 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must mount /tmp with the nosuid option.

```
GROUP ID: V-257868
RULE ID: SV-257868r958804
```

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 "setguid" files. Executing files from untrusted file systems increases the opportunity for nonprivileged users to attain unauthorized administrative access.

Audit:

Verify "/tmp" is mounted with the "nosuid" option:

```
$ mount | grep /tmp

/dev/mapper/rhel-tmp on /tmp type xfs (rw,nodev,nosuid,noexec,seclabel)
```

If the "/tmp" file system is mounted without the "nosuid" option, this is a finding.

Remediation:

Modify "/etc/fstab" to use the "nosuid" option on the "/tmp" directory.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.95 RHEL-09-231140 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must mount /var with the nodev option.

```
GROUP ID: V-257869
RULE ID: SV-257869r958804
```

Rationale:

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for nonprivileged users to attain unauthorized administrative access.

The only legitimate location for device files is the "/dev" directory located on the root partition, with the exception of chroot jails if implemented.

Audit:

Verify "/var" is mounted with the "nodev" option:

```
$ mount | grep /var

/dev/mapper/rhel-var on /var type xfs (rw,nodev,nosuid,noexec,seclabel)
```

If the "/var" file system is mounted without the "nodev" option, this is a finding.

Remediation:

Modify "/etc/fstab" to use the "nodev" option on the "/var" directory.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.96 RHEL-09-231145 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must mount /var/log with the nodev option.

```
GROUP ID: V-257870
RULE ID: SV-257870r958804
```

Rationale:

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for nonprivileged users to attain unauthorized administrative access.

The only legitimate location for device files is the "/dev" directory located on the root partition, with the exception of chroot jails if implemented.

Audit:

Verify "/var/log" is mounted with the "nodev" option:

```
$ mount | grep /var/log

/dev/mapper/rhel-var-log on /var/log type xfs
(rw,nodev,nosuid,noexec,seclabel)
```

If the "/var/log" file system is mounted without the "nodev" option, this is a finding.

Remediation:

Modify "/etc/fstab" to use the "nodev" option on the "/var/log" directory.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.97 RHEL-09-231150 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must mount /var/log with the noexec option.

```
GROUP ID: V-257871
RULE ID: SV-257871r958804
```

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 nonprivileged users to attain unauthorized administrative access.

Audit:

Verify "/var/log" is mounted with the "noexec" option:

```
$ mount | grep /var/log

/dev/mapper/rhel-var-log on /var/log type xfs
(rw,nodev,nosuid,noexec,seclabel)
```

If the "/var/log" file system is mounted without the "noexec" option, this is a finding.

Remediation:

Modify "/etc/fstab" to use the "noexec" option on the "/var/log" directory.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.98 RHEL-09-231155 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must mount /var/log with the nosuid option.

```
GROUP ID: V-257872
RULE ID: SV-257872r958804
```

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 "setguid" files. Executing files from untrusted file systems increases the opportunity for nonprivileged users to attain unauthorized administrative access.

Audit:

Verify "/var/log" is mounted with the "nosuid" option:

```
$ mount | grep /var/log

/dev/mapper/rhel-var-log on /var/log type xfs
(rw,nodev,nosuid,noexec,seclabel)
```

If the "/var/log" file system is mounted without the "nosuid" option, this is a finding.

Remediation:

Modify "/etc/fstab" to use the "nosuid" option on the "/var/log" directory.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.99 RHEL-09-231160 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must mount /var/log/audit with the nodev option.

Rationale:

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for nonprivileged users to attain unauthorized administrative access.

The only legitimate location for device files is the "/dev" directory located on the root partition, with the exception of chroot jails if implemented.

Audit:

Verify "/var/log/audit" is mounted with the "nodev" option:

```
$ mount | grep /var/log/audit

/dev/mapper/rhel-var-log-audit on /var/log/audit type xfs
(rw,nodev,nosuid,noexec,seclabel)
```

If the "/var/log/audit" file system is mounted without the "nodev" option, this is a finding.

Remediation:

Modify "/etc/fstab" to use the "nodev" option on the "/var/log/audit" directory.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.100 RHEL-09-231165 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must mount /var/log/audit with the noexec option.

```
GROUP ID: V-257874
RULE ID: SV-257874r958804
```

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 nonprivileged users to attain unauthorized administrative access.

Audit:

Verify "/var/log/audit" is mounted with the "noexec" option:

```
$ mount | grep /var/log/audit

/dev/mapper/rhel-var-log-audit on /var/log/audit type xfs
(rw,nodev,nosuid,noexec,seclabel)
```

If the "/var/log/audit" file system is mounted without the "noexec" option, this is a finding.

Remediation:

Modify "/etc/fstab" to use the "noexec" option on the "/var/log/audit" directory.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.101 RHEL-09-231170 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must mount /var/log/audit with the nosuid option.

```
GROUP ID: V-257875
RULE ID: SV-257875r958804
```

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 "setguid" files. Executing files from untrusted file systems increases the opportunity for nonprivileged users to attain unauthorized administrative access.

Audit:

Verify "/var/log/audit" is mounted with the "nosuid" option:

```
$ mount | grep /var/log/audit

/dev/mapper/rhel-var-log-audit on /var/log/audit type xfs
(rw,nodev,nosuid,noexec,seclabel)
```

If the "/var/log/audit" file system is mounted without the "nosuid" option, this is a finding.

Remediation:

Modify "/etc/fstab" to use the "nosuid" option on the "/var/log/audit" directory.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.102 RHEL-09-231175 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must mount /var/tmp with the nodev option.

```
GROUP ID: V-257876
RULE ID: SV-257876r958804
```

Rationale:

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for nonprivileged users to attain unauthorized administrative access.

The only legitimate location for device files is the "/dev" directory located on the root partition, with the exception of chroot jails if implemented.

Audit:

Verify "/var/tmp" is mounted with the "nodev" option:

```
$ mount | grep /var/tmp

/dev/mapper/rhel-var-tmp on /var/tmp type xfs
(rw,nodev,nosuid,noexec,seclabel)
```

If the "/var/tmp" file system is mounted without the "nodev" option, this is a finding.

Remediation:

Modify "/etc/fstab" to use the "nodev" option on the "/var/tmp" directory.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.103 RHEL-09-231180 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must mount /var/tmp with the noexec option.

```
GROUP ID: V-257877
RULE ID: SV-257877r958804
```

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 nonprivileged users to attain unauthorized administrative access.

Audit:

Verify "/var/tmp" is mounted with the "noexec" option:

```
$ mount | grep /var/tmp

/dev/mapper/rhel-var-tmp on /var/tmp type xfs
(rw,nodev,nosuid,noexec,seclabel)
```

If the "/var/tmp" file system is mounted without the "noexec" option, this is a finding.

Remediation:

Modify "/etc/fstab" to use the "noexec" option on the "/var/tmp" directory.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.104 RHEL-09-231185 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must mount /var/tmp with the nosuid option.

```
GROUP ID: V-257878
RULE ID: SV-257878r958804
```

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 "setguid" files. Executing files from untrusted file systems increases the opportunity for nonprivileged users to attain unauthorized administrative access.

Audit:

Verify "/var/tmp" is mounted with the "nosuid" option:

```
$ mount | grep /var/tmp

/dev/mapper/rhel-var-tmp on /var/tmp type xfs
(rw,nodev,nosuid,noexec,seclabel)
```

If the "/var/tmp" file system is mounted without the "nosuid" option, this is a finding.

Remediation:

Modify "/etc/fstab" to use the "nosuid" option on the "/var/tmp" directory.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.105 RHEL-09-231190 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

RHEL 9 local disk partitions must implement cryptographic mechanisms to prevent unauthorized disclosure or modification of all information that requires at rest protection.

```
GROUP ID: V-257879
RULE ID: SV-257879r1045454
```

Rationale:

RHEL 9 systems handling data requiring "data at rest" protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest.

Selection of a cryptographic mechanism is based on the need to protect the integrity of organizational information. The strength of the mechanism is commensurate with the security category and/or classification of the information. Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields).

Satisfies: SRG-OS-000405-GPOS-00184, SRG-OS-000185-GPOS-00079, SRG-OS-000404-GPOS-00183

Audit:

Note: If there is a documented and approved reason for not having data-at-rest encryption at the operating system level, such as encryption provided by a hypervisor or a disk storage array in a virtualized environment, this requirement is Not Applicable.
Verify RHEL 9 prevents unauthorized disclosure or modification of all information requiring at-rest protection by using disk encryption.
Note: If there is a documented and approved reason for not having data-at-rest encryption, this requirement is Not Applicable.
List all block devices in tree-like format:

```
$ sudo lsblk --tree

NAME                        MAJ:MIN  RM   SIZE     RO    TYPE    MOUNTPOINTS
zram0                       252:0    0    8G       0     disk    [SWAP]
nvme0n1                     259:0    0    476.9G   0     disk
|-nvme0n1p1                 259:1    0    1G       0     part    /boot/efi
|-nvme0n1p2                 259:2    0    1G       0     part    /boot
|-nvme0n1p3                 259:3    0    474.9G   0     part
  |-luks-<encrypted_id>     253:0    0    474.9G   0     crypt
    |-rhel-root             253:1    0    16G      0     lvm     /
    |-rhel-varcache         253:2    0    8G       0     lvm     /var/cache
    |-rhel-vartmp           253:3    0    4G       0     lvm     /var/tmp
    |-rhel-varlog           253:4    0    4G       0     lvm     /var/log
    |-rhel-home             253:5    0    64G      0     lvm     /home
    |-rhel-varlogaudit      253:6    0    4G       0     lvm
/var/log/audit
```

Verify that the block device tree for each persistent filesystem, excluding the /boot and /boot/efi filesystems, has at least one parent block device of type "crypt", and that the encryption type is LUKS:

```
$ sudo cryptsetup status luks-b74f6910-2547-4399-86b2-8b0252d926d7
/dev/mapper/luks-b74f6910-2547-4399-86b2-8b0252d926d7 is active and is in
use.
  type:    LUKS2
  cipher:  aes-xts-plain64
  keysize: 512 bits
  key location: keyring
  device:  /dev/nvme0n1p3
  sector size:  512
  offset:  32768 sectors
  size:    995986063 sectors
  mode:    read/write
```

If there are persistent filesystems (other than /boot or /boot/efi) whose block device trees do not have a crypt block device of type LUKS, ask the administrator to indicate how persistent filesystems are encrypted.
If there is no evidence that persistent filesystems are encrypted, this is a finding.

Remediation:

Configure RHEL 9 to prevent unauthorized modification of all information at rest by using disk encryption.
Encrypting a partition in an already installed system is more difficult, because existing partitions will need to be resized and changed.
To encrypt an entire partition, dedicate a partition for encryption in the partition layout.

Additional Information:

CCI-001199 Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53 :: SC-28
- NIST SP 800-53 Revision 4 :: SC-28
- NIST SP 800-53 Revision 5 :: SC-28
- NIST SP 800-53A :: SC-28.1

CCI-002475 Implement cryptographic mechanisms to prevent unauthorized modification of organization-defined information when at rest on organization-defined system components.

- NIST SP 800-53 Revision 4 :: SC-28 (1)
- NIST SP 800-53 Revision 5 :: SC-28 (1)

CCI-002476 Implement cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined system components.

- NIST SP 800-53 Revision 4 :: SC-28 (1)
- NIST SP 800-53 Revision 5 :: SC-28 (1)

1.106 RHEL-09-231195 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

RHEL 9 must disable mounting of cramfs.

```
GROUP ID: V-257880
RULE ID: SV-257880r1044951
```

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.

Removing support for unneeded filesystem types reduces the local attack surface of the server.

Compressed ROM/RAM file system (or cramfs) is a read-only file system designed for simplicity and space-efficiency. It is mainly used in embedded and small-footprint systems.

Audit:

Verify that RHEL 9 disables the ability to load the cramfs kernel module with the following command:

```
$ grep -r cramfs /etc/modprobe.conf /etc/modprobe.d/*

install cramfs /bin/false
blacklist cramfs
```

If the command does not return any output or the lines are commented out, and use of cramfs is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Remediation:

To configure the system to prevent the cramfs kernel module from being loaded, add the following lines to the file /etc/modprobe.d/blacklist.conf (or create blacklist.conf if it does not exist):

```
install cramfs /bin/false
blacklist cramfs
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

1.107 RHEL-09-231200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent special devices on non-root local partitions.

```
GROUP ID: V-257881
RULE ID: SV-257881r991589
```

Rationale:

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for nonprivileged users to attain unauthorized administrative access.

The only legitimate location for device files is the "/dev" directory located on the root partition, with the exception of chroot jails if implemented.

Audit:

Verify all non-root local partitions are mounted with the "nodev" option with the following command:

```
$ sudo mount | grep '^/dev\S* on /\S' | grep --invert-match 'nodev'
```

If any output is produced, this is a finding.

Remediation:

Configure the "/etc/fstab" to use the "nodev" option on all non-root local partitions.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.108 RHEL-09-232010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 system commands must have mode 755 or less permissive.

```
GROUP ID: V-257882
RULE ID: SV-257882r991560
```

Rationale:

If RHEL 9 allowed any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to RHEL 9 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges.

Audit:

Verify the system commands contained in the following directories have mode "755" or less permissive with the following command:

```
$ sudo find -L /bin /sbin /usr/bin /usr/sbin /usr/libexec /usr/local/bin
/usr/local/sbin -perm /022 -exec ls -l {} \;
```

If any system commands are found to be group-writable or world-writable, this is a finding.

Remediation:

Configure the system commands to be protected from unauthorized access.
Run the following command, replacing "[FILE]" with any system command with a mode more permissive than "755".

```
$ sudo chmod 755 [FILE]
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53 :: CM-5 (6)
- NIST SP 800-53 Revision 4 :: CM-5 (6)
- NIST SP 800-53 Revision 5 :: CM-5 (6)
- NIST SP 800-53A :: CM-5 (6).1

1.109 RHEL-09-232015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 library directories must have mode 755 or less permissive.

```
GROUP ID: V-257883
RULE ID: SV-257883r991560
```

Rationale:

If RHEL 9 allowed any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to RHEL 9 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges.

Audit:

Verify the system-wide shared library directories have mode "755" or less permissive with the following command:

```
$ sudo find -L /lib /lib64 /usr/lib /usr/lib64 -perm /022 -type d -exec ls -l
{} \;
```

If any system-wide shared library file is found to be group-writable or world-writable, this is a finding.

Remediation:

Configure the system-wide shared library directories (/lib, /lib64, /usr/lib and /usr/lib64) to be protected from unauthorized access.
Run the following command, replacing "[DIRECTORY]" with any library directory with a mode more permissive than 755.

```
$ sudo chmod 755 [DIRECTORY]
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53 :: CM-5 (6)
- NIST SP 800-53 Revision 4 :: CM-5 (6)
- NIST SP 800-53 Revision 5 :: CM-5 (6)
- NIST SP 800-53A :: CM-5 (6).1

1.110 RHEL-09-232020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 library files must have mode 755 or less permissive.

```
GROUP ID: V-257884
RULE ID: SV-257884r991560
```

Rationale:

If RHEL 9 allowed any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to RHEL 9 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges.

Audit:

Verify the system-wide shared library files contained in the following directories have mode "755" or less permissive with the following command:

```
$ sudo find -L /lib /lib64 /usr/lib /usr/lib64 -perm /022 -type f -exec ls -l
{} \;
```

If any system-wide shared library file is found to be group-writable or world-writable, this is a finding.

Remediation:

Configure the library files to be protected from unauthorized access. Run the following command, replacing "[FILE]" with any library file with a mode more permissive than 755.

```
$ sudo chmod 755 [FILE]
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53 :: CM-5 (6)
- NIST SP 800-53 Revision 4 :: CM-5 (6)
- NIST SP 800-53 Revision 5 :: CM-5 (6)
- NIST SP 800-53A :: CM-5 (6).1

1.111 RHEL-09-232025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /var/log directory must have mode 0755 or less permissive.

```
GROUP ID: V-257885
RULE ID: SV-257885r1044953
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the RHEL 9 system or platform. Additionally, personally identifiable information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify that the "/var/log" directory has a mode of "0755" or less permissive with the following command:

```
$ stat -c '%a %n' /var/log

755 /var/log
```

If "/var/log" does not have a mode of "0755" or less permissive, this is a finding.

Remediation:

Configure the "/var/log" directory to a mode of "0755" by running the following command:

```
$ sudo chmod 0755 /var/log
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

1.112 RHEL-09-232030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /var/log/messages file must have mode 0640 or less permissive.

```
GROUP ID: V-257886
RULE ID: SV-257886r1044955
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the RHEL 9 system or platform. Additionally, personally identifiable information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify the "/var/log/messages" file has a mode of "0640" or less permissive with the following command:

```
$ stat -c '%a %n' /var/log/messages

600 /var/log/messages
```

If "/var/log/messages" does not have a mode of "0640" or less permissive, this is a finding.

Remediation:

Configure the "/var/log/messages" file to have a mode of "0640" by running the following command:

```
$ sudo chmod 0640 /var/log/messages
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

1.113 RHEL-09-232035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 audit tools must have a mode of 0755 or less permissive.

```
GROUP ID: V-257887
RULE ID: SV-257887r991557
```

Rationale:

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

RHEL 9 systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools, and the corresponding rights the user enjoys, to make access decisions regarding the access to audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Audit:

Verify the audit tools have a mode of "0755" or less with the following command:

```
$ stat -c "%a %n" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace
/sbin/auditd /sbin/rsyslogd /sbin/augenrules

755 /sbin/auditctl
755 /sbin/aureport
755 /sbin/ausearch
750 /sbin/autrace
755 /sbin/auditd
755 /sbin/rsyslogd
755 /sbin/augenrules
```

If any of the audit tool files have a mode more permissive than "0755", this is a finding.

Remediation:

Configure the audit tools to have a mode of "0755" by running the following command:

```
$ sudo chmod 0755 [audit_tool]
```

Replace "[audit_tool]" with each audit tool that has a more permissive mode than 0755.

Additional Information:

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

1.114 RHEL-09-232040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 permissions of cron configuration files and directories must not be modified from the operating system defaults.

```
GROUP ID: V-257888
RULE ID: SV-257888r1069378
```

Rationale:

If the permissions of cron configuration files or directories are modified from the operating system defaults, it may be possible for individuals to insert unauthorized cron jobs that perform unauthorized actions, including potentially escalating privileges.

Audit:

Run the following command to verify that the owner, group, and mode of cron configuration files and directories match the operating system defaults:

```
$ rpm --verify cronie crontabs | awk '! ($2 == "c" && $1 ~
/^.\..\.\.\.\..\./) {print $0}'
```

If the command returns any output, this is a finding.

Remediation:

Run the following commands to restore the permissions of cron configuration files and directories to the operating system defaults:

```
$ sudo dnf reinstall cronie crontabs
$ rpm --setugids cronie crontabs
$ rpm --setperms cronie crontabs
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.115 RHEL-09-232045 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All RHEL 9 local initialization files must have mode 0740 or less permissive.

```
GROUP ID: V-257889
RULE ID: SV-257889r1044959
```

Rationale:

Local initialization files are used to configure the user's shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Audit:

Verify that all local initialization files have a mode of "0740" or less permissive with the following command:
Note: The example will be for the "bingwa" user, who has a home directory of "/home/bingwa".

```
$ find /home/bingwa/.[^.]* -maxdepth 0 -perm -740 -exec stat -c "%a %n" {} \;
| more

755 /home/bingwa/.somepermissivefile
```

If any local initialization files are returned, this indicates a mode more permissive than "0740", and this is a finding.

Remediation:

Set the mode of the local initialization files to "0740" with the following command:
Note: The example will be for the wadea user, who has a home directory of "/home/wadea".

```
$ sudo chmod 0740 /home/wadea/.<INIT_FILE>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.116 RHEL-09-232050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All RHEL 9 local interactive user home directories must have mode 0750 or less permissive.

```
GROUP ID: V-257890
RULE ID: SV-257890r1044961
```

Rationale:

Excessive permissions on local interactive user home directories may allow unauthorized access to user files by other users.

Audit:

Verify the assigned home directory of all local interactive users has a mode of "0750" or less permissive with the following command:
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.

```
$ stat -L -c '%a %n' $(awk -F: '($3>=1000)&&($7 !~ /nologin/){print $6}'
/etc/passwd) 2>/dev/null

700 /home/bingwa
```

If home directories referenced in "/etc/passwd" do not have a mode of "0750" or less permissive, this is a finding.

Remediation:

Change the mode of interactive user's home directories to "0750". To change the mode of a local interactive user's home directory, use the following command:
Note: The example will be for the user "wadea".

```
$ sudo chmod 0750 /home/wadea
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.117 RHEL-09-232055 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/group file must have mode 0644 or less permissive to prevent unauthorized access.

```
GROUP ID: V-257891
RULE ID: SV-257891r991589
```

Rationale:

Impact:

The "/etc/group" file contains information regarding groups that are configured on the system. Protection of this file is important for system security.

Audit:

Verify that the "/etc/group" file has mode "0644" or less permissive with the following command:

```
$ sudo stat -c "%a %n" /etc/group

644 /etc/group
```

If a value of "0644" or less permissive is not returned, this is a finding.

Remediation:

Change the mode of the file "/etc/group" to "0644" by running the following command:

```
$ sudo chmod 0644 /etc/group
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.118 RHEL-09-232060 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/group- file must have mode 0644 or less permissive to prevent unauthorized access.

```
GROUP ID: V-257892
RULE ID: SV-257892r991589
```

Rationale:

The "/etc/group-" file is a backup file of "/etc/group", and as such, contains information regarding groups that are configured on the system. Protection of this file is important for system security.

Audit:

Verify that the "/etc/group-" file has mode "0644" or less permissive with the following command:

```
$ sudo stat -c "%a %n" /etc/group-

644 /etc/group-
```

If a value of "0644" or less permissive is not returned, this is a finding.

Remediation:

Change the mode of the file "/etc/group-" to "0644" by running the following command:

```
$ sudo chmod 0644 /etc/group-
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.119 RHEL-09-232065 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/gshadow file must have mode 0000 or less permissive to prevent unauthorized access.

```
GROUP ID: V-257893
RULE ID: SV-257893r991589
```

Rationale:

The "/etc/gshadow" file contains group password hashes. Protection of this file is critical for system security.

Audit:

Verify that the "/etc/gshadow" file has mode "0000" with the following command:

```
$ sudo stat -c "%a %n" /etc/gshadow

0 /etc/gshadow
```

If a value of "0" is not returned, this is a finding.

Remediation:

Change the mode of the file "/etc/gshadow" to "0000" by running the following command:

```
$ sudo chmod 0000 /etc/gshadow
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.120 RHEL-09-232070 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/gshadow- file must have mode 0000 or less permissive to prevent unauthorized access.

```
GROUP ID: V-257894
RULE ID: SV-257894r991589
```

Rationale:

The "/etc/gshadow-" file is a backup of "/etc/gshadow", and as such, contains group password hashes. Protection of this file is critical for system security.

Audit:

Verify that the "/etc/gshadow-" file has mode "0000" with the following command:

```
$ sudo stat -c "%a %n" /etc/gshadow-

0 /etc/gshadow-
```

If a value of "0" is not returned, this is a finding.

Remediation:

Default Value:

Change the mode of the file "/etc/gshadow-" to "0000" by running the following command:

```
$ sudo chmod 0000 /etc/gshadow-
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.121 RHEL-09-232075 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/passwd file must have mode 0644 or less permissive to prevent unauthorized access.

```
GROUP ID: V-257895
RULE ID: SV-257895r991589
```

Rationale:

Impact:

If the "/etc/passwd" file is writable by a group-owner or the world the risk of its compromise is increased. The file contains the list of accounts on the system and associated information, and protection of this file is critical for system security.

Audit:

Verify that the "/etc/passwd" file has mode "0644" or less permissive with the following command:

```
$ sudo stat -c "%a %n" /etc/passwd

644 /etc/passwd
```

If a value of "0644" or less permissive is not returned, this is a finding.

Remediation:

Change the mode of the file "/etc/passwd" to "0644" by running the following command:

```
$ sudo chmod 0644 /etc/passwd
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.122 RHEL-09-232080 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/passwd- file must have mode 0644 or less permissive to prevent unauthorized access.

```
GROUP ID: V-257896
RULE ID: SV-257896r991589
```

Rationale:

The "/etc/passwd-" file is a backup file of "/etc/passwd", and as such, contains information about the users that are configured on the system. Protection of this file is critical for system security.

Audit:

Verify that the "/etc/passwd-" file has mode "0644" or less permissive with the following command:

```
$ sudo stat -c "%a %n" /etc/passwd-

644 /etc/passwd-
```

If a value of "0644" or less permissive is not returned, this is a finding.

Remediation:

Change the mode of the file "/etc/passwd-" to "0644" by running the following command:

```
$ sudo chmod 0644 /etc/passwd-
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.123 RHEL-09-232085 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/shadow- file must have mode 0000 or less permissive to prevent unauthorized access.

```
GROUP ID: V-257897
RULE ID: SV-257897r991589
```

Rationale:

The "/etc/shadow-" file is a backup file of "/etc/shadow", and as such, contains the list of local system accounts and password hashes. Protection of this file is critical for system security.

Audit:

Verify that the "/etc/shadow-" file has mode "0000" with the following command:

```
$ sudo stat -c "%a %n" /etc/shadow-

0 /etc/shadow-
```

If a value of "0" is not returned, this is a finding.

Remediation:

Change the mode of the file "/etc/shadow-" to "0000" by running the following command:

```
$ sudo chmod 0000 /etc/shadow-
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.124 RHEL-09-232090 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/group file must be owned by root.

```
GROUP ID: V-257898
RULE ID: SV-257898r991589
```

Rationale:

The "/etc/group" file contains information regarding groups that are configured on the system. Protection of this file is important for system security.

Audit:

Verify the ownership of the "/etc/group" file with the following command:

```
$ sudo stat -c "%U %n" /etc/group

root /etc/group
```

If "/etc/group" file does not have an owner of "root", this is a finding.

Remediation:

Change the owner of the file /etc/group to root by running the following command:

```
$ sudo chown root /etc/group
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.125 RHEL-09-232095 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/group file must be group-owned by root.

```
GROUP ID: V-257899
RULE ID: SV-257899r991589
```

Rationale:

The "/etc/group" file contains information regarding groups that are configured on the system. Protection of this file is important for system security.

Audit:

Verify the group ownership of the "/etc/group" file with the following command:

```
$ sudo stat -c "%G %n" /etc/group

root /etc/group
```

If "/etc/group" file does not have a group owner of "root", this is a finding.

Remediation:

Change the group of the file /etc/group to root by running the following command:

```
$ sudo chgrp root /etc/group
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.126 RHEL-09-232100 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/group- file must be owned by root.

```
GROUP ID: V-257900
RULE ID: SV-257900r991589
```

Rationale:

The "/etc/group-" file is a backup file of "/etc/group", and as such, contains information regarding groups that are configured on the system. Protection of this file is important for system security.

Audit:

Verify the ownership of the "/etc/group-" file with the following command:

```
$ sudo stat -c "%U %n" /etc/group-

root /etc/group-
```

If "/etc/group-" file does not have an owner of "root", this is a finding.

Remediation:

Change the owner of the file /etc/group- to root by running the following command:

```
$ sudo chown root /etc/group-
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.127 RHEL-09-232103 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 "/etc/audit/" must be owned by root.

```
GROUP ID: V-270175
RULE ID: SV-270175r1044964
```

Rationale:

The "/etc/audit/" directory contains files that ensure the proper auditing of command execution, privilege escalation, file manipulation, and more. Protection of this directory is critical for system security.

Audit:

Verify the ownership of the "/etc/audit/" directory with the following command:

```
$ sudo stat -c "%U %n" /etc/audit/

root /etc/audit/
```

If the "/etc/audit/" directory does not have an owner of "root", this is a finding.

Remediation:

Change the owner of the file "/etc/audit/" to "root" by running the following command:

```
$ sudo chown root /etc/audit/
```

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

1.128 RHEL-09-232104 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 "/etc/audit/" must be group-owned by root.

```
GROUP ID: V-270176
RULE ID: SV-270176r1044967
```

Rationale:

The "/etc/audit/" directory contains files that ensure the proper auditing of command execution, privilege escalation, file manipulation, and more. Protection of this directory is critical for system security.

Audit:

Verify the group ownership of the "/etc/audit/" directory with the following command:

```
$ sudo stat -c "%G %n" /etc/audit/

root /etc/audit/
```

If "/etc/audit/" does not have a group owner of "root", this is a finding.

Remediation:

Change the group of the file "/etc/audit/" to "root" by running the following command:

```
$ sudo chgrp root /etc/audit/
```

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

1.129 RHEL-09-232105 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/group- file must be group-owned by root.

```
GROUP ID: V-257901
RULE ID: SV-257901r991589
```

Rationale:

The "/etc/group-" file is a backup file of "/etc/group", and as such, contains information regarding groups that are configured on the system. Protection of this file is important for system security.

Audit:

Verify the group ownership of the "/etc/group-" file with the following command:

```
$ sudo stat -c "%G %n" /etc/group-

root /etc/group-
```

If "/etc/group-" file does not have a group owner of "root", this is a finding.

Remediation:

Change the group of the file /etc/group- to root by running the following command:

```
$ sudo chgrp root /etc/group-
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.130 RHEL-09-232110 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/gshadow file must be owned by root.

```
GROUP ID: V-257902
RULE ID: SV-257902r991589
```

Rationale:

The "/etc/gshadow" file contains group password hashes. Protection of this file is critical for system security.

Audit:

Verify the ownership of the "/etc/gshadow" file with the following command:

```
$ sudo stat -c "%U %n" /etc/gshadow

root /etc/gshadow
```

If "/etc/gshadow" file does not have an owner of "root", this is a finding.

Remediation:

Change the owner of the file /etc/gshadow to root by running the following command:

```
$ sudo chown root /etc/gshadow
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.131 RHEL-09-232115 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/gshadow file must be group-owned by root.

```
GROUP ID: V-257903
RULE ID: SV-257903r991589
```

Rationale:

The "/etc/gshadow" file contains group password hashes. Protection of this file is critical for system security.

Audit:

Verify the group ownership of the "/etc/gshadow" file with the following command:

```
$ sudo stat -c "%G %n" /etc/gshadow

root /etc/gshadow
```

If "/etc/gshadow" file does not have a group owner of "root", this is a finding.

Remediation:

Change the group of the file /etc/gshadow to root by running the following command:

```
$ sudo chgrp root /etc/gshadow
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.132 RHEL-09-232120 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/gshadow- file must be owned by root.

```
GROUP ID: V-257904
RULE ID: SV-257904r991589
```

Rationale:

The "/etc/gshadow-" file is a backup of "/etc/gshadow", and as such, contains group password hashes. Protection of this file is critical for system security.

Audit:

Verify the ownership of the "/etc/gshadow-" file with the following command:

```
$ sudo stat -c "%U %n" /etc/gshadow-

root /etc/gshadow-
```

If "/etc/gshadow-" file does not have an owner of "root", this is a finding.

Remediation:

Default Value:

Change the owner of the file /etc/gshadow- to root by running the following command:

```
$ sudo chown root /etc/gshadow-
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.133 RHEL-09-232125 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/gshadow- file must be group-owned by root.

```
GROUP ID: V-257905
RULE ID: SV-257905r991589
```

Rationale:

The "/etc/gshadow-" file is a backup of "/etc/gshadow", and as such, contains group password hashes. Protection of this file is critical for system security.

Audit:

Verify the group ownership of the "/etc/gshadow-" file with the following command:

```
$ sudo stat -c "%G %n" /etc/gshadow-

root /etc/gshadow-
```

If "/etc/gshadow-" file does not have a group owner of "root", this is a finding.

Remediation:

Default Value:

Change the group of the file /etc/gshadow- to root by running the following command:

```
$ sudo chgrp root /etc/gshadow-
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.134 RHEL-09-232130 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/passwd file must be owned by root.

```
GROUP ID: V-257906
RULE ID: SV-257906r991589
```

Rationale:

The "/etc/passwd" file contains information about the users that are configured on the system. Protection of this file is critical for system security.

Audit:

Verify the ownership of the "/etc/passwd" file with the following command:

```
$ sudo stat -c "%U %n" /etc/passwd

root /etc/passwd
```

If "/etc/passwd" file does not have an owner of "root", this is a finding.

Remediation:

Change the owner of the file /etc/passwd to root by running the following command:

```
$ sudo chown root /etc/passwd
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.135 RHEL-09-232135 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/passwd file must be group-owned by root.

```
GROUP ID:V-257907
RULE ID: SV-257907r991589
```

Rationale:

The "/etc/passwd" file contains information about the users that are configured on the system. Protection of this file is critical for system security.

Audit:

Verify the group ownership of the "/etc/passwd" file with the following command:

```
$ sudo stat -c "%G %n" /etc/passwd

root /etc/passwd
```

If "/etc/passwd" file does not have a group owner of "root", this is a finding.

Remediation:

Default Value:

Change the group of the file /etc/passwd to root by running the following command:

```
$ sudo chgrp root /etc/passwd
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.136 RHEL-09-232140 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/passwd- file must be owned by root.

```
GROUP ID: V-257908
RULE ID: SV-257908r991589
```

Rationale:

The "/etc/passwd-" file is a backup file of "/etc/passwd", and as such, contains information about the users that are configured on the system. Protection of this file is critical for system security.

Audit:

Verify the ownership of the "/etc/passwd-" file with the following command:

```
$ sudo stat -c "%U %n" /etc/passwd-

root /etc/passwd-
```

If "/etc/passwd-" file does not have an owner of "root", this is a finding.

Remediation:

Default Value:

Change the owner of the file /etc/passwd- to root by running the following command:

```
$ sudo chown root /etc/passwd-
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.137 RHEL-09-232145 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/passwd- file must be group-owned by root.

```
GROUP ID: V-257909
RULE ID: SV-257909r991589
```

Rationale:

The "/etc/passwd-" file is a backup file of "/etc/passwd", and as such, contains information about the users that are configured on the system. Protection of this file is critical for system security.

Audit:

Verify the group ownership of the "/etc/passwd-" file with the following command:

```
$ sudo stat -c "%G %n" /etc/passwd-

root /etc/passwd-
```

If "/etc/passwd-" file does not have a group owner of "root", this is a finding.

Remediation:

Change the group of the file /etc/passwd- to root by running the following command:

```
$ sudo chgrp root /etc/passwd-
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.138 RHEL-09-232150 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/shadow file must be owned by root.

```
GROUP ID: V-257910
RULE ID: SV-257910r991589
```

Rationale:

Impact:

The "/etc/shadow" file contains the list of local system accounts and stores password hashes. Protection of this file is critical for system security. Failure to give ownership of this file to root provides the designated owner with access to sensitive information, which could weaken the system security posture.

Audit:

Verify the ownership of the "/etc/shadow" file with the following command:

```
$ sudo stat -c "%U %n" /etc/shadow

root /etc/shadow
```

If "/etc/shadow" file does not have an owner of "root", this is a finding.

Remediation:

Default Value:

Change the owner of the file /etc/shadow to root by running the following command:

```
$ sudo chown root /etc/shadow
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.139 RHEL-09-232155 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/shadow file must be group-owned by root.

```
GROUP ID: V-257911
RULE ID: SV-257911r991589
```

Rationale:

The "/etc/shadow" file stores password hashes. Protection of this file is critical for system security.

Audit:

Verify the group ownership of the "/etc/shadow" file with the following command:

```
$ sudo stat -c "%G %n" /etc/shadow

root /etc/shadow
```

If "/etc/shadow" file does not have a group owner of "root", this is a finding.

Remediation:

Change the group of the file /etc/shadow to root by running the following command:

```
$ sudo chgrp root /etc/shadow
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.140 RHEL-09-232160 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/shadow- file must be owned by root.

```
GROUP ID: V-257912
RULE ID: SV-257912r991589
```

Rationale:

The "/etc/shadow-" file is a backup file of "/etc/shadow", and as such, contains the list of local system accounts and password hashes. Protection of this file is critical for system security.

Audit:

Verify the ownership of the "/etc/shadow-" file with the following command:

```
$ sudo stat -c "%U %n" /etc/shadow-

root /etc/shadow-
```

If "/etc/shadow-" file does not have an owner of "root", this is a finding.

Remediation:

Change the owner of the file /etc/shadow- to root by running the following command:

```
$ sudo chown root /etc/shadow-
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.141 RHEL-09-232165 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/shadow- file must be group-owned by root.

```
GROUP ID: V-257913
RULE ID: SV-257913r991589
```

Rationale:

The "/etc/shadow-" file is a backup file of "/etc/shadow", and as such, contains the list of local system accounts and password hashes. Protection of this file is critical for system security.

Audit:

Verify the group ownership of the "/etc/shadow-" file with the following command:

```
$ sudo stat -c "%G %n" /etc/shadow-

root /etc/shadow-
```

If "/etc/shadow-" file does not have a group owner of "root", this is a finding.

Remediation:

Change the group of the file /etc/shadow- to root by running the following command:

```
$ sudo chgrp root /etc/shadow-
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.142 RHEL-09-232170 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /var/log directory must be owned by root.

```
GROUP ID: V-257914
RULE ID: SV-257914r1044969
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the RHEL 9 system or platform. Additionally, personally identifiable information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify the "/var/log" directory is owned by root with the following command:

```
$ stat -c "%U %n" /var/log

root /var/log
```

If "/var/log" does not have an owner of "root", this is a finding.

Remediation:

Configure the owner of the directory "/var/log" to "root" by running the following command:

```
$ sudo chown root /var/log
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

1.143 RHEL-09-232175 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /var/log directory must be group-owned by root.

GROUP ID: V-257915 RULE ID: SV-257915r1044971

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the RHEL 9 system or platform. Additionally, personally identifiable information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify the "/var/log" directory is group-owned by root with the following command:

```
$ stat -c "%G %n" /var/log

root /var/log
```

If "/var/log" does not have a group owner of "root", this is a finding.

Remediation:

Configure the group owner of the directory "/var/log" to "root" by running the following command:

```
$ sudo chgrp root /var/log
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

1.144 RHEL-09-232180 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /var/log/messages file must be owned by root.

```
GROUP ID: V-257916
RULE ID: SV-257916r1044973
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the RHEL 9 system or platform. Additionally, personally identifiable information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify the "/var/log/messages" file is owned by root with the following command:

```
$ stat -c "%U %n" /var/log/messages

root /var/log
```

If "/var/log/messages" does not have an owner of "root", this is a finding.

Remediation:

Change the owner of the "/var/log/messages" file to "root" by running the following command:

```
$ sudo chown root /var/log/messages
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

1.145 RHEL-09-232185 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /var/log/messages file must be group-owned by root.

```
GROUP ID: V-257917
RULE ID: SV-257917r1044975
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the RHEL 9 system or platform. Additionally, personally identifiable information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify the "/var/log/messages" file is group-owned by root with the following command:

```
$ stat -c "%G %n" /var/log/messages

root /var/log
```

If "/var/log/messages" does not have a group owner of "root", this is a finding.

Remediation:

Change the group owner of the "/var/log/messages" file to "root" by running the following command:

```
$ sudo chgrp root /var/log/messages
```

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

1.146 RHEL-09-232190 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 system commands must be owned by root.

```
GROUP ID: V-257918
RULE ID: SV-257918r1044977
```

Rationale:

If RHEL 9 allowed any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to RHEL 9 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges.

Audit:

Verify the system commands contained in the following directories are owned by "root" with the following command:

```
$ sudo find -L /bin /sbin /usr/bin /usr/sbin /usr/libexec /usr/local/bin
/usr/local/sbin ! -user root -exec stat -L -c "%U %n" {} \;
```

If any system commands are found to not be owned by root, this is a finding.

Remediation:

Configure the system commands to be protected from unauthorized access.
Run the following command, replacing "[FILE]" with any system command file not owned by "root".

```
$ sudo chown root [FILE]
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53 :: CM-5 (6)
- NIST SP 800-53 Revision 4 :: CM-5 (6)
- NIST SP 800-53 Revision 5 :: CM-5 (6)
- NIST SP 800-53A :: CM-5 (6).1

1.147 RHEL-09-232195 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 system commands must be group-owned by root or a system account.

```
GROUP ID: V-257919
RULE ID: SV-257919r1044979
```

Rationale:

If RHEL 9 allowed any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to RHEL 9 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges.

Audit:

Verify the system commands contained in the following directories are group-owned by "root", or a required system account, with the following command:

```
$ sudo find -L /bin /sbin /usr/bin /usr/sbin /usr/libexec /usr/local/bin
/usr/local/sbin ! -group root -exec stat -L -c "%G %n" {} \;
```

If any system commands are returned and are not group-owned by a required system account, this is a finding.

Remediation:

Configure the system commands to be protected from unauthorized access.
Run the following command, replacing "[FILE]" with any system command file not group-owned by "root" or a required system account.

```
$ sudo chgrp root [FILE]
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53 :: CM-5 (6)
- NIST SP 800-53 Revision 4 :: CM-5 (6)
- NIST SP 800-53 Revision 5 :: CM-5 (6)
- NIST SP 800-53A :: CM-5 (6).1

1.148 RHEL-09-232200 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 library files must be owned by root.

```
GROUP ID: V-257920
RULE ID: SV-257920r1069385
```

Rationale:

If RHEL 9 allowed any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to RHEL 9 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges.

Audit:

Verify the systemwide shared library files are owned by "root" with the following command:

```
$ sudo find -L /lib /lib64 /usr/lib /usr/lib64 ! -user root ! -type d -exec
stat -L -c "%U %n" {} \;
```

If any systemwide shared library file is not owned by root, this is a finding.

Remediation:

Configure the systemwide shared library files (/lib, /lib64, /usr/lib and /usr/lib64) to be protected from unauthorized access.
Run the following command, replacing "[FILE]" with any library file not owned by "root".

```
$ sudo chown root [FILE]
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53 :: CM-5 (6)
- NIST SP 800-53 Revision 4 :: CM-5 (6)
- NIST SP 800-53 Revision 5 :: CM-5 (6)
- NIST SP 800-53A :: CM-5 (6).1

1.149 RHEL-09-232205 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 library files must be group-owned by root or a system account.

```
GROUP ID: V-257921
RULE ID: SV-257921r1069387
```

Rationale:

If RHEL 9 allowed any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to RHEL 9 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges.

Audit:

Verify the systemwide shared library files are group-owned by "root" with the following command:

```
$ sudo find -L /lib /lib64 /usr/lib /usr/lib64 ! -group root ! -type d -exec
stat -L -c "%G %n" {} \;
```

If any systemwide shared library file is returned and is not group-owned by a required system account, this is a finding.

Remediation:

Configure the systemwide shared library files (/lib, /lib64, /usr/lib and /usr/lib64) to be protected from unauthorized access.
Run the following command, replacing "[FILE]" with any library file not group-owned by "root".

```
$ sudo chgrp root [FILE]
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53 :: CM-5 (6)
- NIST SP 800-53 Revision 4 :: CM-5 (6)
- NIST SP 800-53 Revision 5 :: CM-5 (6)
- NIST SP 800-53A :: CM-5 (6).1

1.150 RHEL-09-232210 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 library directories must be owned by root.

```
GROUP ID: V-257922
RULE ID: SV-257922r1044988
```

Rationale:

If RHEL 9 allowed any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to RHEL 9 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges.

Audit:

Verify the systemwide shared library directories are owned by "root" with the following command:

```
$ sudo find /lib /lib64 /usr/lib /usr/lib64 ! -user root -type d -exec stat -
c "%U %n" {} \;
```

If any systemwide shared library directory is not owned by "root", this is a finding.

Remediation:

Configure the systemwide shared library directories within (/lib, /lib64, /usr/lib and /usr/lib64) to be protected from unauthorized access.
Run the following command, replacing "[DIRECTORY]" with any library directory not owned by "root".

```
$ sudo chown root [DIRECTORY]
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53 :: CM-5 (6)
- NIST SP 800-53 Revision 4 :: CM-5 (6)
- NIST SP 800-53 Revision 5 :: CM-5 (6)
- NIST SP 800-53A :: CM-5 (6).1

1.151 RHEL-09-232215 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 library directories must be group-owned by root or a system account.

```
GROUP ID: V-257923
RULE ID: SV-257923r1044991
```

Rationale:

If RHEL 9 allowed any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to RHEL 9 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges.

Audit:

Verify the systemwide shared library directories are group-owned by "root" with the following command:

```
$ sudo find /lib /lib64 /usr/lib /usr/lib64 ! -group root -type d -exec stat
-c "%G %n" {} \;
```

If any systemwide shared library directory is returned and is not group-owned by a required system account, this is a finding.

Remediation:

Configure the systemwide shared library directories (/lib, /lib64, /usr/lib and /usr/lib64) to be protected from unauthorized access.
Run the following command, replacing "[DIRECTORY]" with any library directory not group-owned by "root".

```
$ sudo chgrp root [DIRECTORY]
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53 :: CM-5 (6)
- NIST SP 800-53 Revision 4 :: CM-5 (6)
- NIST SP 800-53 Revision 5 :: CM-5 (6)
- NIST SP 800-53A :: CM-5 (6).1

1.152 RHEL-09-232220 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 audit tools must be owned by root.

```
GROUP ID: V-257924
RULE ID: SV-257924r99155
```

Rationale:

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

RHEL 9 systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools, and the corresponding rights the user enjoys, to make access decisions regarding the access to audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Audit:

Verify the audit tools are owned by "root" with the following command:

```
$ sudo stat -c "%U %n" /sbin/auditctl /sbin/aureport /sbin/ausearch
/sbin/autrace /sbin/auditd /sbin/rsyslogd /sbin/augenrules

root /sbin/auditctl
root /sbin/aureport
root /sbin/ausearch
root /sbin/autrace
root /sbin/auditd
root /sbin/rsyslogd
root /sbin/augenrules
```

If any audit tools do not have an owner of "root", this is a finding.

Remediation:

Configure the audit tools to be owned by "root" by running the following command:

```
$ sudo chown root [audit_tool]
```

Replace "[audit_tool]" with each audit tool not owned by "root".

Additional Information:

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

1.153 RHEL-09-232225 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 audit tools must be group-owned by root.

```
GROUP ID: V-257925
RULE ID: SV-257925r991557
```

Rationale:

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data; therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

RHEL 9 systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools, and the corresponding rights the user enjoys, to make access decisions regarding the access to audit tools.

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Audit:

Verify the audit tools are group owned by "root" with the following command:

```
$ sudo stat -c "%G %n" /sbin/auditctl /sbin/aureport /sbin/ausearch
/sbin/autrace /sbin/auditd /sbin/rsyslogd /sbin/augenrules

root /sbin/auditctl
root /sbin/aureport
root /sbin/ausearch
root /sbin/autrace
root /sbin/auditd
root /sbin/rsyslogd
root /sbin/augenrules
```

If any audit tools do not have a group owner of "root", this is a finding.

Remediation:

Configure the audit tools to be group-owned by "root" by running the following command:

```
$ sudo chgrp root [audit_tool]
```

Replace "[audit_tool]" with each audit tool not group-owned by "root".

Additional Information:

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

1.154 RHEL-09-232230 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 cron configuration files directory must be owned by root.

```
GROUP ID: V-257926
RULE ID: SV-257926r991589
```

Rationale:

Service configuration files enable or disable features of their respective services that if configured incorrectly can lead to insecure and vulnerable configurations; therefore, service configuration files must be owned by the correct group to prevent unauthorized changes.

Audit:

Verify the ownership of all cron configuration files with the command:

```
$ stat -c "%U %n" /etc/cron*

root /etc/cron.d
root /etc/cron.daily
root /etc/cron.deny
root /etc/cron.hourly
root /etc/cron.monthly
root /etc/crontab
root /etc/cron.weekly
```

If any crontab is not owned by root, this is a finding.

Remediation:

Configure any cron configuration not owned by root with the following command:

```
$ sudo chown root [cron config file]
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.155 RHEL-09-232235 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 cron configuration files directory must be group-owned by root.

```
GROUP ID: V-257927
RULE ID: SV-257927r991589
```

Rationale:

Service configuration files enable or disable features of their respective services that if configured incorrectly can lead to insecure and vulnerable configurations; therefore, service configuration files should be owned by the correct group to prevent unauthorized changes.

Audit:

Verify the group ownership of all cron configuration files with the following command:

```
$ stat -c "%G %n" /etc/cron*

root /etc/cron.d
root /etc/cron.daily
root /etc/cron.deny
root /etc/cron.hourly
root /etc/cron.monthly
root /etc/crontab
root /etc/cron.weekly
```

If any crontab is not group owned by root, this is a finding.

Remediation:

Configure any cron configuration not group-owned by root with the following command:

```
$ sudo chgrp root [cron config file]
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.156 RHEL-09-232240 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All RHEL 9 world-writable directories must be owned by root, sys, bin, or an application user.

```
GROUP ID: V-257928
RULE ID: SV-257928r1044992
```

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.

Satisfies: SRG-OS-000480-GPOS-00227, SRG-OS-000138-GPOS-00069

Audit:

Verify that world writable directories are owned by root, a system account, or an application account with the following command. It will discover and print world-writable directories that are not owned by root. Run it once for each local partition [PART]:

```
$ sudo find  PART  -xdev -type d -perm -0002 -uid +0 -print
```

If there is output, this is a finding.

Remediation:

Configure all public directories to be owned by root or a system account to prevent unauthorized and unintended information transferred via shared system resources.
Set the owner of all public directories as root or a system account using the command, replace "[Public Directory]" with any directory path not owned by root or a system account:

```
$ sudo chown root [Public Directory]
```

Additional Information:

CCI-001090 Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53 :: SC-4
- NIST SP 800-53 Revision 4 :: SC-4
- NIST SP 800-53 Revision 5 :: SC-4
- NIST SP 800-53A :: SC-4.1

1.157 RHEL-09-232245 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

A sticky bit must be set on all RHEL 9 public directories.

```
GROUP ID: V-257929
RULE ID: SV-257929r958524
```

Rationale:

Preventing unauthorized information transfers mitigates the risk of information, including encrypted representations of information, produced by the actions of prior users/roles (or the actions of processes acting on behalf of prior users/roles) from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems. The control of information in shared resources is also commonly referred to as object reuse and residual information protection.

This requirement generally applies to the design of an information technology product, but it can also apply to the configuration of particular information system components that are, or use, such products. This can be verified by acceptance/validation processes in DOD or other government agencies.

Audit:

Verify that all world-writable directories have the sticky bit set.
Determine if all world-writable directories have the sticky bit set by running the following command:

```
$ sudo find / -type d \( -perm -0002 -a ! -perm -1000 \) -print 2>/dev/null

drwxrwxrwt 7 root root 4096 Jul 26 11:19 /tmp
```

If any of the returned directories are world-writable and do not have the sticky bit set, this is a finding.

Remediation:

Configure all world-writable directories to have the sticky bit set to prevent unauthorized and unintended information transferred via shared system resources.
Set the sticky bit on all world-writable directories using the command, replace "[World-Writable Directory]" with any directory path missing the sticky bit:

```
$ chmod a+t [World-Writable Directory]
```

Additional Information:

CCI-001090 Prevent unauthorized and unintended information transfer via shared system resources.

- NIST SP 800-53 :: SC-4
- NIST SP 800-53 Revision 4 :: SC-4
- NIST SP 800-53 Revision 5 :: SC-4
- NIST SP 800-53A :: SC-4.1

1.158 RHEL-09-232250 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

All RHEL 9 local files and directories must have a valid group owner.

```
GROUP ID: V-257930
RULE ID: SV-257930r991589
```

Rationale:

Files without a valid group owner may be unintentionally inherited if a group is assigned the same Group Identifier (GID) as the GID of the files without a valid group owner.

Audit:

Verify all local files and directories on RHEL 9 have a valid group with the following command:

```
$ df --local -P | awk {'if (NR!=1) print $6'} | sudo xargs -I '{}' find '{}'
-xdev -nogroup
```

If any files on the system do not have an assigned group, this is a finding.

Remediation:

Either remove all files and directories from RHEL 9 that do not have a valid group, or assign a valid group to all files and directories on the system with the "chgrp" command:

```
$ sudo chgrp <group> <file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.159 RHEL-09-232255 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

All RHEL 9 local files and directories must have a valid owner.

```
GROUP ID: V-257931
RULE ID: SV-257931r991589
```

Rationale:

Unowned files and directories may be unintentionally inherited if a user is assigned the same user identifier "UID" as the UID of the unowned files.

Audit:

Verify all local files and directories on RHEL 9 have a valid owner with the following command:

```
$ df --local -P | awk {'if (NR!=1) print $6'} | sudo xargs -I '{}' find '{}'
-xdev -nouser
```

If any files on the system do not have an assigned owner, this is a finding.

Remediation:

Either remove all files and directories from the system that do not have a valid user, or assign a valid user to all unowned files and directories on RHEL 9 with the "chown" command:

```
$ sudo chown <user> <file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.160 RHEL-09-232260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must be configured so that all system device files are correctly labeled to prevent unauthorized modification.

```
GROUP ID: V-257932
RULE ID: SV-257932r1014838
```

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, this is a finding.

Remediation:

Restore the SELinux policy for the affected device file from the system policy database using the following command:

```
$ sudo restorecon -v <device_path>
```

Substitute "<device_path>" with the path to the affected device file (from the output of the previous commands). An example device file path would be "/dev/ttyUSB0". If the output of the above command does not indicate that the device was relabeled to a more specific SELinux type label, then the SELinux policy of the system must be updated with more specific policy for the device class specified. If a package was used to install support for a device class, that package could be reinstalled using the following command:

```
$ sudo dnf reinstall <package_name>
```

If a package was not used to install the SELinux policy for a given device class, then it must be generated manually and provide specific type labels.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.161 RHEL-09-232270 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/shadow file must have mode 0000 to prevent unauthorized access.

```
GROUP ID: V-257934
RULE ID: SV-257934r991589
```

Rationale:

The "/etc/shadow" file contains the list of local system accounts and stores password hashes. Protection of this file is critical for system security. Failure to give ownership of this file to root provides the designated owner with access to sensitive information, which could weaken the system security posture.

Audit:

Verify that the "/etc/shadow" file has mode "0000" with the following command:

```
$ sudo stat -c "%a %n" /etc/shadow

0 /etc/shadow
```

If a value of "0" is not returned, this is a finding.

Remediation:

Change the mode of the file "/etc/shadow" to "0000" by running the following command:

```
$ sudo chmod 0000 /etc/shadow
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.162 RHEL-09-251010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must have the firewalld package installed.

```
GROUP ID: V-257935
RULE ID: SV-257935r1044994
```

Rationale:

"Firewalld" provides an easy and effective way to block/limit remote access to the system via ports, services, and protocols.

Remote access services, such as those providing remote access to network devices and information systems, which lack automated control capabilities, increase risk and make remote user access management difficult at best.

Remote access is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

RHEL 9 functionality (e.g., SSH) must be capable of taking enforcement action if the audit reveals unauthorized activity. Automated control of remote access sessions allows organizations to ensure ongoing compliance with remote access policies by enforcing connection rules of remote access applications on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

Satisfies: SRG-OS-000096-GPOS-00050, SRG-OS-000297-GPOS-00115, SRG-OS-000298-GPOS-00116, SRG-OS-000480-GPOS-00227, SRG-OS-000480-GPOS-00232

Audit:

Run the following command to determine if the firewalld package is installed with the following command:

```
$ dnf list --installed firewalld
```

Example output:

```
firewalld.noarch          1.0.0-4.el9
```

If the "firewall" package is not installed, this is a finding.

Remediation:

To install the "firewalld" package run the following command:

```
$ sudo dnf install firewalld
```

Additional Information:

CCI-000382 Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 b
- NIST SP 800-53 Revision 5 :: CM-7 b
- NIST SP 800-53A :: CM-7.1 (iii)

CCI-002314 Employ automated mechanisms to control remote access methods.

- NIST SP 800-53 Revision 4 :: AC-17 (1)
- NIST SP 800-53 Revision 5 :: AC-17 (1)

CCI-002322 Provide the capability to disconnect or disable remote access to the system within the organization-defined time period.

- NIST SP 800-53 Revision 4 :: AC-17 (9)
- NIST SP 800-53 Revision 5 :: AC-17 (9)

1.163 RHEL-09-251015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The firewalld service on RHEL 9 must be active.

```
GROUP ID: V-257936
RULE ID: SV-257936r1044995
```

Rationale:

"Firewalld" provides an easy and effective way to block/limit remote access to the system via ports, services, and protocols.

Remote access services, such as those providing remote access to network devices and information systems, which lack automated control capabilities, increase risk and make remote user access management difficult at best.

Remote access is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

RHEL 9 functionality (e.g., RDP) must be capable of taking enforcement action if the audit reveals unauthorized activity. Automated control of remote access sessions allows organizations to ensure ongoing compliance with remote access policies by enforcing connection rules of remote access applications on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

Satisfies: SRG-OS-000096-GPOS-00050, SRG-OS-000297-GPOS-00115, SRG-OS-000480-GPOS-00227, SRG-OS-000480-GPOS-00232

Audit:

Verify that "firewalld" is active with the following command:

```
$ systemctl is-active firewalld

active
```

If the firewalld service is not active, this is a finding.

Remediation:

To enable the firewalld service run the following command:

```
$ sudo systemctl enable --now firewalld
```

Additional Information:

CCI-000382 Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 b
- NIST SP 800-53 Revision 5 :: CM-7 b
- NIST SP 800-53A :: CM-7.1 (iii)

CCI-002314 Employ automated mechanisms to control remote access methods.

- NIST SP 800-53 Revision 4 :: AC-17 (1)
- NIST SP 800-53 Revision 5 :: AC-17 (1)

1.164 RHEL-09-251020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

A RHEL 9 firewall must employ a deny-all, allow-by-exception policy for allowing connections to other systems.

```
GROUP ID: V-257937
RULE ID: SV-257937r991589
```

Rationale:

Failure to restrict network connectivity only to authorized systems permits inbound connections from malicious systems. It also permits outbound connections that may facilitate exfiltration of DOD data.

RHEL 9 incorporates the "firewalld" daemon, which allows for many different configurations. One of these configurations is zones. Zones can be utilized to a deny-all, allow-by-exception approach. The default "drop" zone will drop all incoming network packets unless it is explicitly allowed by the configuration file or is related to an outgoing network connection.

Audit:

Verify the RHEL 9 "firewalld" is configured to employ a deny-all, allow-by-exception policy for allowing connections to other systems with the following commands:

```
$ sudo  firewall-cmd --state


running

$ sudo firewall-cmd --get-active-zones

public
   interfaces: ens33

$ sudo firewall-cmd --info-zone=public | grep target

   target: DROP

$ sudo firewall-cmd --permanent --info-zone=public | grep target

   target: DROP
```

If no zones are active on the RHEL 9 interfaces or if runtime and permanent targets are set to a different option other than "DROP", this is a finding.

Remediation:

Configure the "firewalld" daemon to employ a deny-all, allow-by-exception with the following commands:
Start by adding the exceptions that are required for mission functionality to the "drop" zone. If SSH access on port 22 is needed, for example, run the following:

```
$ sudo firewall-cmd --permanent --add-service=ssh --zone=drop
```

Reload the firewall rules to update the runtime configuration from the "--permanent" changes made above:

```
$ sudo firewall-cmd --reload
```

Set the default zone to the drop zone:

```
$ sudo firewall-cmd --set-default-zone=drop
```

Note: This is a runtime and permanent change.
Add any interfaces to the newly modified "drop" zone:

```
$ sudo firewall-cmd --permanent --zone=drop --change-interface=ens33
```

Reload the firewall rules for changes to take effect:

```
$ sudo firewall-cmd --reload
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.165 RHEL-09-251030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must protect against or limit the effects of denial-of-service (DoS) attacks by ensuring rate-limiting measures on impacted network interfaces are implemented.

```
GROUP ID: V-257939
RULE ID: SV-257939r1044997
```

Rationale:

DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of RHEL 9 to mitigate the impact of DoS attacks that have occurred or are ongoing on system availability. For each system, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exists to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or establishing memory partitions). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

Audit:

Verify "nftables" is configured to allow rate limits on any connection to the system with the following command:

```
$ sudo grep -i firewallbackend /etc/firewalld/firewalld.conf

# FirewallBackend
FirewallBackend=nftables
```

If the "nftables" is not set as the "FirewallBackend" default, this is a finding.

Remediation:

Configure "nftables" to be the default "firewallbackend" for "firewalld" by adding or editing the following line in "/etc/firewalld/firewalld.conf":

```
FirewallBackend=nftables
```

Establish rate-limiting rules based on organization-defined types of DoS attacks on impacted network interfaces.

Additional Information:

CCI-002385 Protect against or limit the effects of organization-defined types of denial of service events.

- NIST SP 800-53 Revision 4 :: SC-5
- NIST SP 800-53 Revision 5 :: SC-5 a

1.166 RHEL-09-251035 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the Ports, Protocols, and Services Management (PPSM) Category Assignments List (CAL) and vulnerability assessments.

```
GROUP ID: V-257940
RULE ID: SV-257940r958480
```

Rationale:

To prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary ports, protocols, and services on information systems.

Audit:

Inspect the firewall configuration and running services to verify it is configured to prohibit or restrict the use of functions, ports, protocols, and/or services that are unnecessary or prohibited.
Check which services are currently active with the following command:

```
$ sudo firewall-cmd --list-all-zones

custom (active)
target: DROP
icmp-block-inversion: no
interfaces: ens33
sources:
services: dhcpv6-client dns http https ldaps rpc-bind ssh
ports:
masquerade: no
forward-ports:
icmp-blocks:
rich rules:
```

Ask the system administrator for the site or program Ports, Protocols, and Services Management Component Local Service Assessment (PPSM CLSA). Verify the services allowed by the firewall match the PPSM CLSA.
If there are additional ports, protocols, or services that are not in the PPSM CLSA, or there are ports, protocols, or services that are prohibited by the PPSM Category Assurance List (CAL), this is a finding.

Remediation:

Update the host's firewall settings and/or running services to comply with the PPSM CLSA for the site or program and the PPSM CAL.
Then run the following command to load the newly created rule(s):

```
$ sudo firewall-cmd --reload
```

Additional Information:

CCI-000382 Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 b
- NIST SP 800-53 Revision 5 :: CM-7 b
- NIST SP 800-53A :: CM-7.1 (iii)

1.167 RHEL-09-251040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 network interfaces must not be in promiscuous mode.

```
GROUP ID: V-257941
RULE ID: SV-257941r991589
```

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 systems security officer (ISSO) and restricted to only authorized personnel.

Audit:

Verify network interfaces are not in promiscuous mode with the following command:

```
$ ip link | grep -i promisc
```

If network interfaces are found on the system in promiscuous mode and their use has not been approved by the ISSO and documented, this is a finding.

Remediation:

Configure network interfaces to turn off promiscuous mode unless approved by the ISSO and documented.
Set the promiscuous mode of an interface to off with the following command:

```
$ sudo ip link set dev <devicename> multicast off promisc off
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.168 RHEL-09-251045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must enable hardening for the Berkeley Packet Filter just-in-time compiler.

```
GROUP ID: V-257942
RULE ID: SV-257942r1044999
```

Rationale:

When hardened, the extended Berkeley Packet Filter (BPF) just-in-time (JIT) compiler will randomize any kernel addresses in the BPF programs and maps, and will not expose the JIT addresses in "/proc/kallsyms".

Audit:

Verify RHEL 9 enables hardening for the BPF JIT with the following commands:

```
$ sudo sysctl net.core.bpf_jit_harden

net.core.bpf_jit_harden = 2
```

If the returned line does not have a value of "2", or a line is not returned, this is a finding.
Check that the configuration files are present to enable this kernel parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F net.core.bpf_jit_harden | tail -1

net.core.bpf_jit_harden = 2
```

If the network parameter "net.core.bpf_jit_harden" is not equal to "2" or nothing is returned, this is a finding.

Remediation:

Configure RHEL 9 to enable hardening for the BPF JIT compiler by adding the following line to a file, in the "/etc/sysctl.d" directory:

```
net.core.bpf_jit_harden = 2
```

The system configuration files need to be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.169 RHEL-09-252010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must have the chrony package installed.

```
GROUP ID: V-257943
RULE ID: SV-257943r1045001
```

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.

Audit:

Verify that RHEL 9 has the chrony package installed with the following command:

```
$ dnf list --installed chrony
```

Example output:

```
chrony.x86_64          4.1-3.el9
```

If the "chrony" package is not installed, this is a finding.

Remediation:

The chrony package can be installed with the following command:

```
$ sudo dnf install chrony
```

Additional Information:

CCI-004923 Compare the internal system clocks on an organization-defined frequency with organization-defined authoritative time source.

- NIST SP 800-53 Revision 5 :: SC-45 (1) (a)

CCI-001891 The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source.

- NIST SP 800-53 Revision 4 :: AU-8 (1) (a)

1.170 RHEL-09-252015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 chronyd service must be enabled.

```
GROUP ID: V-257944
RULE ID: SV-257944r1038944
```

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.

Audit:

Verify the chronyd service is active with the following command:

```
$ systemctl is-active chronyd

active
```

If the chronyd service is not active, this is a finding.

Remediation:

To enable the chronyd service run the following command:

```
$ sudo systemctl enable --now chronyd
```

Additional Information:

CCI-004923 Compare the internal system clocks on an organization-defined frequency with organization-defined authoritative time source.

- NIST SP 800-53 Revision 5 :: SC-45 (1) (a)

CCI-001891 The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source.

- NIST SP 800-53 Revision 4 :: AU-8 (1) (a)

1.171 RHEL-09-252020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must securely compare internal information system clocks at least every 24 hours.

```
GROUP ID: V-257945
RULE ID: SV-257945r1038944
```

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.

Depending on the infrastructure being used the "pool" directive may not be supported.

Authoritative time sources include the 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).

Satisfies: SRG-OS-000355-GPOS-00143, SRG-OS-000356-GPOS-00144, SRG-OS-000359-GPOS-00146

Audit:

Verify RHEL 9 is securely comparing internal information system clocks at least every 24 hours with an NTP server with the following commands:

```
$ sudo grep maxpoll /etc/chrony.conf

server 0.us.pool.ntp.mil iburst maxpoll 16
```

If the "maxpoll" option is set to a number greater than 16 or the line is commented out, this is a finding.
Verify the "chrony.conf" file is configured to an authoritative DOD time source by running the following command:

```
$ sudo grep -i server /etc/chrony.conf
server 0.us.pool.ntp.mil
```

If the parameter "server" is not set or is not set to an authoritative DOD time source, this is a finding.

Remediation:

Configure RHEL 9 to securely compare internal information system clocks at least every 24 hours with an NTP server by adding/modifying the following line in the /etc/chrony.conf file.

```
server [ntp.server.name] iburst maxpoll 16
```

Additional Information:

CCI-001890 Record time stamps for audit records that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

- NIST SP 800-53 Revision 4 :: AU-8 b
- NIST SP 800-53 Revision 5 :: AU-8 b

CCI-004923 Compare the internal system clocks on an organization-defined frequency with organization-defined authoritative time source.

- NIST SP 800-53 Revision 5 :: SC-45 (1) (a)

CCI-004926 Synchronize the internal system clocks to the authoritative time source when the time difference is greater than organization-defined time period.

- NIST SP 800-53 Revision 5 :: SC-45 (1) (b)

CCI-001891 The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source.

- NIST SP 800-53 Revision 4 :: AU-8 (1) (a)

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.

- NIST SP 800-53 Revision 4 :: AU-8 (1) (b)

1.172 RHEL-09-252025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must disable the chrony daemon from acting as a server.

```
GROUP ID: V-257946
RULE ID: SV-257946r958480
```

Rationale:

Minimizing the exposure of the server functionality of the chrony daemon diminishes the attack surface.

Satisfies: SRG-OS-000096-GPOS-00050, SRG-OS-000095-GPOS-00049

Audit:

Verify RHEL 9 disables the chrony daemon from acting as a server with the following command:

```
$ grep -w port /etc/chrony.conf

port 0
```

If the "port" option is not set to "0", is commented out, or is missing, this is a finding.

Remediation:

Configure RHEL 9 to disable the chrony daemon from acting as a server by adding/modifying the following line in the /etc/chrony.conf file:

```
port 0
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

CCI-000382 Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 b
- NIST SP 800-53 Revision 5 :: CM-7 b
- NIST SP 800-53A :: CM-7.1 (iii)

1.173 RHEL-09-252030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must disable network management of the chrony daemon.

```
GROUP ID: V-257947
RULE ID: SV-257947r958480
```

Rationale:

Not exposing the management interface of the chrony daemon on the network diminishes the attack space.

Satisfies: SRG-OS-000096-GPOS-00050, SRG-OS-000095-GPOS-00049

Audit:

Verify RHEL 9 disables network management of the chrony daemon with the following command:

```
$ grep -w cmdport /etc/chrony.conf

cmdport 0
```

If the "cmdport" option is not set to "0", is commented out, or is missing, this is a finding.

Remediation:

Configure RHEL 9 to disable network management of the chrony daemon by adding/modifying the following line in the /etc/chrony.conf file:

```
cmdport 0
```

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

CCI-000382 Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 b
- NIST SP 800-53 Revision 5 :: CM-7 b
- NIST SP 800-53A :: CM-7.1 (iii)

1.174 RHEL-09-252035 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 systems using Domain Name Servers (DNS) resolution must have at least two name servers configured.

```
GROUP ID: V-257948
RULE ID: SV-257948r1045004
```

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:

Note: If the system is running in a cloud platform and the cloud provider gives a single, highly available IP address for DNS configuration, this control is Not Applicable.
Verify 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 fewer than two lines are returned that are not commented out, this is a finding.

Remediation:

Configure the operating system to use two or more name servers for DNS resolution based on the DNS mode of the system.
If the NetworkManager DNS mode is set to "none", add the following lines to "/etc/resolv.conf":

```
nameserver [name server 1]
nameserver [name server 2]
```

Replace [name server 1] and [name server 2] with the IPs of two different DNS resolvers.
If the NetworkManager DNS mode is set to "default", add two DNS servers to a NetworkManager connection using the following command:

```
$ nmcli connection modify [connection name] ipv4.dns [name server 1],[name
server 2]
```

Replace [name server 1] and [name server 2] with the IPs of two different DNS resolvers. Replace [connection name] with a valid NetworkManager connection name on the system. Replace ipv4 with ipv6 if IPv6 DNS servers are used.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.175 RHEL-09-252040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must configure a DNS processing mode in Network Manager.

```
GROUP ID: V-257949
RULE ID: SV-257949r1014841
```

Rationale:

In order to ensure that DNS resolver settings are respected, a DNS mode in Network Manager must be configured.

Audit:

Verify that RHEL 9 has a DNS mode configured in Network Manager.

```
$ NetworkManager --print-config
[main]
dns=none
```

If the dns key under main does not exist or is not set to "none" or "default", this is a finding.
Note: If RHEL 9 is configured to use a DNS resolver other than Network Manager, the configuration must be documented and approved by the information system security officer (ISSO).

Remediation:

Configure NetworkManager in RHEL 9 to use a DNS mode.
In "/etc/NetworkManager/NetworkManager.conf" add the following line in the "[main]" section:

```
dns = none
```

NetworkManager must be reloaded for the change to take effect.

```
$ sudo systemctl reload NetworkManager
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.176 RHEL-09-252045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not have unauthorized IP tunnels configured.

```
GROUP ID: V-257950
RULE ID: SV-257950r1045006
```

Rationale:

IP tunneling mechanisms can be used to bypass network filtering. If tunneling is required, it must be documented with the information system security officer (ISSO).

Audit:

Verify that RHEL 9 does not have unauthorized IP tunnels configured.
Determine if the "IPsec" service is active with the following command:

```
$ systemctl is-active ipsec

Inactive
```

If the "IPsec" service is active, check for configured IPsec connections ("conn"), with the following command:

```
$ sudo grep -rni conn /etc/ipsec.conf /etc/ipsec.d/
```

Verify any returned results are documented with the ISSO.
If the IPsec tunnels are active and not approved, this is a finding.

Remediation:

Remove all unapproved tunnels from the system, or document them with the ISSO.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.177 RHEL-09-252050 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must be configured to prevent unrestricted mail relaying.

```
GROUP ID: V-257951
RULE ID: SV-257951r1014843
```

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:

If postfix is not installed, this is Not Applicable.
Verify RHEL 9 is configured to prevent unrestricted mail relaying 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", and the additional entries have not been documented with the information system security officer (ISSO), this is a finding.

Remediation:

Modify the postfix configuration file to restrict client connections to the local network with the following command:

```
$ sudo postconf -e 'smtpd_client_restrictions = permit_mynetworks,reject'
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.178 RHEL-09-252060 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must forward mail from postmaster to the root account using a postfix alias.

```
GROUP ID: V-257953
RULE ID: SV-257953r958424
```

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.

Audit:

Verify that the administrators are notified in the event of an audit processing failure. Check that the "/etc/aliases" file has a defined value for "root".

```
$ sudo grep "postmaster:\s*root$" /etc/aliases
```

If the command does not return a line, or the line is commented out, ask the system administrator to indicate how they and the information systems security officer (ISSO) are notified of an audit process failure. If there is no evidence of the proper personnel being notified of an audit processing failure, this is a finding.

Remediation:

Configure a valid email address as an alias for the root account.
Append the following line to "/etc/aliases":

```
postmaster: root
```

Then, run the following command:

```
$ sudo newaliases
```

Additional Information:

CCI-000139 Alert organization-defined personnel or roles within an organization-defined time period in the event of an audit logging process failure.

- NIST SP 800-53 :: AU-5 a
- NIST SP 800-53 Revision 4 :: AU-5 a
- NIST SP 800-53 Revision 5 :: AU-5 a
- NIST SP 800-53A :: AU-5.1 (ii)

1.179 RHEL-09-252065 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 libreswan package must be installed.

```
GROUP ID: V-257954
RULE ID: SV-257954r1045008
```

Rationale:

Providing the ability for remote users or systems to initiate a secure VPN connection protects information when it is transmitted over a wide area network.

Satisfies: SRG-OS-000480-GPOS-00227, SRG-OS-000120-GPOS-00061

Audit:

Verify that RHEL 9 libreswan service package is installed.
Check that the libreswan service package is installed with the following command:

```
$ dnf list --installed libreswan
```

Example output:

```
libreswan.x86_64          4.6-3.el9
```

If the "libreswan" package is not installed, this is a finding.

Remediation:

Install the libreswan service (if it is not already installed) with the following command:

```
$ sudo dnf install libreswan
```

Additional Information:

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53 :: IA-7
- NIST SP 800-53 Revision 4 :: IA-7
- NIST SP 800-53 Revision 5 :: IA-7
- NIST SP 800-53A :: IA-7.1

1.180 RHEL-09-252070 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

There must be no shosts.equiv files on RHEL 9.

```
GROUP ID: V-257955
RULE ID: SV-257955r991589
```

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 RHEL 9 with the following command:

```
$ sudo find / -name shosts.equiv
```

If a "shosts.equiv" file is found, this is a finding.

Remediation:

Remove any found "shosts.equiv" files from the system.

```
$ sudo rm /[path]/[to]/[file]/shosts.equiv
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.181 RHEL-09-252075 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

There must be no .shosts files on RHEL 9.

```
GROUP ID: V-257956
RULE ID: SV-257956r991589
```

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 RHEL 9 with the following command:

```
$ sudo find / -name .shosts
```

If a ".shosts" file is found, this is a finding.

Remediation:

Remove any found ".shosts" files from the system.

```
$ sudo rm /[path]/[to]/[file]/.shosts
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.182 RHEL-09-253010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must be configured to use TCP syncookies.

```
GROUP ID: V-257957
RULE ID: SV-257957r1045009
```

Rationale:

Denial of service (DoS) is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

Managing excess capacity ensures that sufficient capacity is available to counter flooding attacks. Employing increased capacity and service redundancy may reduce the susceptibility to some DoS attacks. Managing excess capacity may include, for example, establishing selected usage priorities, quotas, or partitioning.

Satisfies: SRG-OS-000480-GPOS-00227, SRG-OS-000420-GPOS-00186, SRG-OS-000142-GPOS-00071

Audit:

Verify RHEL 9 is configured to use IPv4 TCP syncookies.
Determine if syncookies are used with the following command:
Check the status of the kernel.perf_event_paranoid kernel parameter.

```
$ sudo sysctl net.ipv4.tcp_syncookies

net.ipv4.tcp_syncookies = 1
```

Check that the configuration files are present to enable this kernel parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F net.ipv4.tcp_syncookies | tail -1

net.ipv4.tcp_syncookies = 1
```

If the network parameter "ipv4.tcp_syncookies" is not equal to "1" or nothing is returned, this is a finding.

Remediation:

Configure RHEL 9 to use TCP syncookies.
Add or edit the following line in a system configuration file in the "/etc/sysctl.d/" directory:

```
net.ipv4.tcp_syncookies = 1
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

- NIST SP 800-53 :: SC-5 (2)
- NIST SP 800-53 Revision 4 :: SC-5 (2)
- NIST SP 800-53 Revision 5 :: SC-5 (2)
- NIST SP 800-53A :: SC-5 (2).1

CCI-002385 Protect against or limit the effects of organization-defined types of denial of service events.

- NIST SP 800-53 Revision 4 :: SC-5
- NIST SP 800-53 Revision 5 :: SC-5 a

1.183 RHEL-09-253015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must ignore Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages.

```
GROUP ID: V-257958
RULE ID: SV-257958r991589
```

Rationale:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

This feature of the IPv4 protocol has few legitimate uses. It should be disabled unless absolutely required.

Audit:

Verify RHEL 9 will not accept IPv4 ICMP redirect messages.
Check the value of the all "accept_redirects" variables with the following command:

```
$ sudo sysctl net.ipv4.conf.all.accept_redirects

net.ipv4.conf.all.accept_redirects = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.
Check that the configuration files are present to enable this network parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F net.ipv4.conf.all.accept_redirects | tail -1

net.ipv4.conf.all.accept_redirects = 0
```

If "net.ipv4.conf.all.accept_redirects" is not set to "0" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to ignore IPv4 ICMP redirect messages.
Add or edit the following line in a single system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv4.conf.all.accept_redirects = 0
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.184 RHEL-09-253020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not forward Internet Protocol version 4 (IPv4) source-routed packets.

```
GROUP ID: V-257959
RULE ID: SV-257959r991589
```

Rationale:

Source-routed packets allow the source of the packet to suggest routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routerd traffic, such as when IPv4 forwarding is enabled and the system is functioning as a router.

Accepting source-routed packets in the IPv4 protocol has few legitimate uses. It must be disabled unless it is absolutely required.

Audit:

Verify RHEL 9 will not accept IPv4 source-routed packets.
Check the value of the all "accept_source_route" variables with the following command:

```
$ sudo sysctl net.ipv4.conf.all.accept_source_route

net.ipv4.conf.all.accept_source_route = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.
Check that the configuration files are present to enable this network parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F net.ipv4.conf.all.accept_source_route | tail -1

net.ipv4.conf.all.accept_source_route = 0
```

If "net.ipv4.conf.all.accept_source_route" is not set to "0" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to ignore IPv4 source-routed packets.
Add or edit the following line in a single system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv4.conf.all.accept_source_route = 0
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.185 RHEL-09-253025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must log IPv4 packets with impossible addresses.

```
GROUP ID: V-257960
RULE ID: SV-257960r991589
```

Rationale:

The presence of "martian" packets (which have impossible addresses) as well as spoofed packets, source-routed packets, and redirects could be a sign of nefarious network activity. Logging these packets enables this activity to be detected.

Audit:

Verify RHEL 9 logs IPv4 martian packets.
Check the value of the accept source route variable with the following command:

```
$ sudo sysctl net.ipv4.conf.all.log_martians

net.ipv4.conf.all.log_martians = 1
```

If the returned line does not have a value of "1", a line is not returned, or the line is commented out, this is a finding.
Check that the configuration files are present to enable this network parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F net.ipv4.conf.all.log_martians | tail -1

net.ipv4.conf.all.log_martians = 1
```

If "net.ipv4.conf.all.log_martians" is not set to "1" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to log martian packets on IPv4 interfaces.
Add or edit the following line in a single system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv4.conf.all.log_martians=1
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.186 RHEL-09-253030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must log IPv4 packets with impossible addresses by default.

GROUP ID: V-257961 RULE ID: SV-257961r991589

Rationale:

The presence of "martian" packets (which have impossible addresses) as well as spoofed packets, source-routed packets, and redirects could be a sign of nefarious network activity. Logging these packets enables this activity to be detected.

Audit:

Verify RHEL 9 logs IPv4 martian packets by default.
Check the value of the accept source route variable with the following command:

```
$ sudo sysctl net.ipv4.conf.default.log_martians

net.ipv4.conf.default.log_martians = 1
```

If the returned line does not have a value of "1", a line is not returned, or the line is commented out, this is a finding.
Check that the configuration files are present to enable this network parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F net.ipv4.conf.default.log_martians | tail -1

net.ipv4.conf.default.log_martians = 1
```

If "net.ipv4.conf.default.log_martians" is not set to "1" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to log martian packets on IPv4 interfaces by default.
Add or edit the following line in a single system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv4.conf.default.log_martians=1
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.187 RHEL-09-253035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must use reverse path filtering on all IPv4 interfaces.

```
GROUP ID: V-257962
RULE ID: SV-257962r991589
```

Rationale:

Enabling reverse path filtering drops packets with source addresses that should not have been able to be received on the interface on which they were received. It must not be used on systems that are routers for complicated networks, but is helpful for end hosts and routers serving small networks.

Audit:

Verify RHEL 9 uses reverse path filtering on all IPv4 interfaces with the following commands:

```
$ sudo sysctl net.ipv4.conf.all.rp_filter

net.ipv4.conf.all.rp_filter = 1
```

If the returned line does not have a value of "1", or a line is not returned, this is a finding.
Check that the configuration files are present to enable this network parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F net.ipv4.conf.all.rp_filter | tail -1

net.ipv4.conf.all.rp_filter = 1
```

If "net.ipv4.conf.all.rp_filter" is not set to "1" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to use reverse path filtering on all IPv4 interfaces.
Add or edit the following line in a single system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv4.conf.all.rp_filter = 1
```

The system configuration files need to be reloaded for the changes to take effect. To reload the contents of the files, run the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.188 RHEL-09-253040 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent IPv4 Internet Control Message Protocol (ICMP) redirect messages from being accepted.

```
GROUP ID: V-257963
RULE ID: SV-257963r991589
```

Rationale:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

This feature of the IPv4 protocol has few legitimate uses. It must be disabled unless absolutely required.

Audit:

Verify RHEL 9 will not accept IPv4 ICMP redirect messages.
Check the value of the default "accept_redirects" variables with the following command:

```
$ sudo sysctl net.ipv4.conf.default.accept_redirects

net.ipv4.conf.default.accept_redirects = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.
Check that the configuration files are present to enable this network parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F net.ipv4.conf.default.accept_redirects | tail -1

net.ipv4.conf.default.accept_redirects = 0
```

If "net.ipv4.conf.default.accept_redirects" is not set to "0" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to prevent IPv4 ICMP redirect messages from being accepted.
Add or edit the following line in a single system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv4.conf.default.accept_redirects = 0
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.189 RHEL-09-253045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not forward IPv4 source-routed packets by default.

```
GROUP ID: V-257964
RULE ID: SV-257964r991589
```

Rationale:

Source-routed packets allow the source of the packet to suggest routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures.

Accepting source-routed packets in the IPv4 protocol has few legitimate uses. It must be disabled unless it is absolutely required, such as when IPv4 forwarding is enabled and the system is legitimately functioning as a router.

Audit:

Verify RHEL 9 does not accept IPv4 source-routed packets by default.
Check the value of the accept source route variable with the following command:

```
$ sudo sysctl net.ipv4.conf.default.accept_source_route

net.ipv4.conf.default.accept_source_route = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.
Check that the configuration files are present to enable this network parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F net.ipv4.conf.default.accept_source_route | tail -1

net.ipv4.conf.default.accept_source_route = 0
```

If "net.ipv4.conf.default.accept_source_route" is not set to "0" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to not forward IPv4 source-routed packets by default.
Add or edit the following line in a single system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv4.conf.default.accept_source_route = 0
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.190 RHEL-09-253050 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must use a reverse-path filter for IPv4 network traffic when possible by default.

```
GROUP ID: V-257965
RULE ID: SV-257965r991589
```

Rationale:

Enabling reverse path filtering drops packets with source addresses that should not have been able to be received on the interface on which they were received. It must not be used on systems that are routers for complicated networks, but is helpful for end hosts and routers serving small networks.

Audit:

Verify RHEL 9 uses reverse path filtering on IPv4 interfaces with the following commands:

```
$ sudo sysctl net.ipv4.conf.default.rp_filter

net.ipv4.conf.default.rp_filter = 1
```

If the returned line does not have a value of "1", or a line is not returned, this is a finding.
Check that the configuration files are present to enable this network parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F net.ipv4.conf.default.rp_filter | tail -1

net.ipv4.conf.default.rp_filter = 1
```

If "net.ipv4.conf.default.rp_filter" is not set to "1" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to use reverse path filtering on IPv4 interfaces by default.
Add or edit the following line in a single system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv4.conf.default.rp_filter = 1
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.191 RHEL-09-253055 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not respond to Internet Control Message Protocol (ICMP) echoes sent to a broadcast address.

```
GROUP ID: V-257966
RULE ID: SV-257966r991589
```

Rationale:

Responding to broadcast (ICMP) echoes facilitates network mapping and provides a vector for amplification attacks.

Ignoring ICMP echo requests (pings) sent to broadcast or multicast addresses makes the system slightly more difficult to enumerate on the network.

Audit:

Verify RHEL 9 does not respond to ICMP echoes sent to a broadcast address.
Check the value of the "icmp_echo_ignore_broadcasts" variable with the following command:

```
$ sudo sysctl net.ipv4.icmp_echo_ignore_broadcasts

net.ipv4.icmp_echo_ignore_broadcasts = 1
```

If the returned line does not have a value of "1", a line is not returned, or the retuned line is commented out, this is a finding.
Check that the configuration files are present to enable this network parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|$)' |
grep -F net.ipv4.icmp_echo_ignore_broadcasts | tail -1

net.ipv4.icmp_echo_ignore_broadcasts = 1
```

If "net.ipv4.icmp_echo_ignore_broadcasts" is not set to "1" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to not respond to IPv4 ICMP echoes sent to a broadcast address. Add or edit the following line in a single system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.192 RHEL-09-253060 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must limit the number of bogus Internet Control Message Protocol (ICMP) response errors logs.

```
GROUP ID: V-257967
RULE ID: SV-257967r991589
```

Rationale:

Some routers will send responses to broadcast frames that violate RFC-1122, which fills up a log file system with many useless error messages. An attacker may take advantage of this and attempt to flood the logs with bogus error logs. Ignoring bogus ICMP error responses reduces log size, although some activity would not be logged.

Audit:

The runtime status of the net.ipv4.icmp_ignore_bogus_error_responses kernel parameter can be queried by running the following command:

```
$ sudo sysctl net.ipv4.icmp_ignore_bogus_error_responses

net.ipv4.icmp_ignore_bogus_error_responses = 1
```

If "net.ipv4.icmp_ignore_bogus_error_responses" is not set to "1", this is a finding.
Check that the configuration files are present to enable this network parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F net.ipv4.icmp_ignore_bogus_error_response | tail -1

net.ipv4.icmp_ignore_bogus_error_response = 1
```

If "net.ipv4.icmp_ignore_bogus_error_response" is not set to "1" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to not log bogus ICMP errors:
Add or edit the following line in a single system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv4.icmp_ignore_bogus_error_responses = 1
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.193 RHEL-09-253065 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not send Internet Control Message Protocol (ICMP) redirects.

```
GROUP ID: V-257968
RULE ID: SV-257968r991589
```

Rationale:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the system's route table possibly revealing portions of the network topology.

The ability to send ICMP redirects is only appropriate for systems acting as routers.

Audit:

Verify RHEL 9 does not IPv4 ICMP redirect messages.
Check the value of the "all send_redirects" variables with the following command:

```
$ sudo sysctl net.ipv4.conf.all.send_redirects

net.ipv4.conf.all.send_redirects = 0
```

If the returned line does not have a value of "0", or a line is not returned, this is a finding.
Check that the configuration files are present to enable this network parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F net.ipv4.conf.all.send_redirects | tail -1

net.ipv4.conf.all.send_redirects = 0
```

If "net.ipv4.conf.all.send_redirects" is not set to "0" and is not documented with the information system security officer (ISSO) as an operational requirement or is missing, this is a finding.

Remediation:

Configure RHEL 9 to not allow interfaces to perform IPv4 ICMP redirects.
Add or edit the following line in a single system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv4.conf.all.send_redirects = 0
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.194 RHEL-09-253070 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not allow interfaces to perform Internet Control Message Protocol (ICMP) redirects by default.

```
GROUP ID: V-257969
RULE ID: SV-257969r991589
```

Rationale:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the system's route table possibly revealing portions of the network topology.

The ability to send ICMP redirects is only appropriate for systems acting as routers.

Audit:

Verify RHEL 9 does not allow interfaces to perform Internet Protocol version 4 (IPv4) ICMP redirects by default.
Check the value of the "default send_redirects" variables with the following command:

```
$ sudo sysctl net.ipv4.conf.default.send_redirects

net.ipv4.conf.default.send_redirects=0
```

If the returned line does not have a value of "0", or a line is not returned, this is a finding.
Check that the configuration files are present to enable this network parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F net.ipv4.conf.default.send_redirects | tail -1

net.ipv4.conf.default.send_redirects = 0
```

If "net.ipv4.conf.default.send_redirects" is not set to "0" and is not documented with the information system security officer (ISSO) as an operational requirement or is missing, this is a finding.

Remediation:

Configure RHEL 9 to not allow interfaces to perform Internet Protocol version 4 (IPv4) ICMP redirects by default.
Add or edit the following line in a single system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv4.conf.default.send_redirects = 0
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.195 RHEL-09-253075 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not enable IPv4 packet forwarding unless the system is a router.

```
GROUP ID: V-257970
RULE ID: SV-257970r1045011
```

Rationale:

Routing protocol daemons are typically used on routers to exchange network topology information with other routers. If this capability is used when not required, system network information may be unnecessarily transmitted across the network.

Audit:

Verify RHEL 9 is not performing IPv4 packet forwarding unless the system is a router. Check that IPv4 forwarding is disabled using the following command:

```
$ sudo sysctl net.ipv4.conf.all.forwarding

net.ipv4.conf.all.forwarding = 0
```

If the IPv4 forwarding value is not "0" and is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.
Check that the configuration files are present to enable this network parameter.

```
$ /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|$)' | grep -F
net.ipv4.conf.all.forwarding | tail -1

net.ipv4.conf.all.forwarding = 0
```

If "net.ipv4.conf.all.forwarding" is not set to "0" and is not documented with the ISSO as an operational requirement or is missing, this is a finding.

Remediation:

Configure RHEL 9 to not allow IPv4 packet forwarding, unless the system is a router. Add or edit the following line in a single system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv4.conf.all.forwarding = 0
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.196 RHEL-09-254010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not accept router advertisements on all IPv6 interfaces.

```
GROUP ID: V-257971
RULE ID: SV-257971r991589
```

Rationale:

An illicit router advertisement message could result in a man-in-the-middle attack.

Audit:

Verify RHEL 9 does not accept router advertisements on all IPv6 interfaces, unless the system is a router.
Note: If IPv6 is disabled on the system, this requirement is Not Applicable.
Determine if router advertisements are not accepted by using the following command:

```
$ sudo sysctl net.ipv6.conf.all.accept_ra

net.ipv6.conf.all.accept_ra = 0
```

If the "accept_ra" value is not "0" and is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.
Check that the configuration files are present to enable this network parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F net.ipv6.conf.all.accept_ra | tail -1

net.ipv6.conf.all.accept_ra = 0
```

If "net.ipv6.conf.all.accept_ra" is not set to "0" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to not accept router advertisements on all IPv6 interfaces unless the system is a router.
Add or edit the following line in a single system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv6.conf.all.accept_ra = 0
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.197 RHEL-09-254015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must ignore IPv6 Internet Control Message Protocol (ICMP) redirect messages.

```
GROUP ID: V-257972
RULE ID: SV-257972r991589
```

Rationale:

An illicit ICMP redirect message could result in a man-in-the-middle attack.

Audit:

Verify RHEL 9 ignores IPv6 ICMP redirect messages.
Note: If IPv6 is disabled on the system, this requirement is Not Applicable.
Check the value of the "accept_redirects" variables with the following command:

```
$ sysctl net.ipv6.conf.all.accept_redirects

net.ipv6.conf.all.accept_redirects = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.
Check that the configuration files are present to enable this network parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F net.ipv6.conf.all.accept_redirects | tail -1

net.ipv6.conf.all.accept_redirects = 0
```

If "net.ipv6.conf.all.accept_redirects" is not set to "0" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to ignore IPv6 ICMP redirect messages.
Add or edit the following line in a single system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv6.conf.all.accept_redirects = 0
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.198 RHEL-09-254020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not forward IPv6 source-routed packets.

```
GROUP ID: V-257973
RULE ID: SV-257973r991589
```

Rationale:

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when forwarding is enabled and the system is functioning as a router.

Audit:

Verify RHEL 9 does not accept IPv6 source-routed packets.
Note: If IPv6 is disabled on the system, this requirement is Not Applicable.
Check the value of the accept source route variable with the following command:

```
$ sudo sysctl net.ipv6.conf.all.accept_source_route

net.ipv6.conf.all.accept_source_route = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.
Check that the configuration files are present to enable this network parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F net.ipv6.conf.all.accept_source_route | tail -1

net.ipv6.conf.all.accept_source_route = 0
```

If "net.ipv6.conf.all.accept_source_route" is not set to "0" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to not forward IPv6 source-routed packets.
Add or edit the following line in a single system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv6.conf.all.accept_source_route = 0
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.199 RHEL-09-254025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not enable IPv6 packet forwarding unless the system is a router.

```
GROUP ID: V-257974
RULE ID: SV-257974r991589
```

Rationale:

IP forwarding permits the kernel to forward packets from one network interface to another. The ability to forward packets between two networks is only appropriate for systems acting as routers.

Audit:

Verify RHEL 9 is not performing IPv6 packet forwarding, unless the system is a router.
Note: If IPv6 is disabled on the system, this requirement is Not Applicable.
Check that IPv6 forwarding is disabled using the following commands:

```
$ sudo sysctl net.ipv6.conf.all.forwarding

net.ipv6.conf.all.forwarding = 0
```

If the IPv6 forwarding value is not "0" and is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.
Check that the configuration files are present to enable this network parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F net.ipv6.conf.all.forwarding | tail -1

net.ipv6.conf.all.forwarding = 0
```

If "net.ipv6.conf.all.forwarding" is not set to "0" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to not allow IPv6 packet forwarding, unless the system is a router. Add or edit the following line in a single system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv6.conf.all.forwarding = 0
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.200 RHEL-09-254030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not accept router advertisements on all IPv6 interfaces by default.

```
GROUP ID: V-257975
RULE ID: SV-257975r991589
```

Rationale:

An illicit router advertisement message could result in a man-in-the-middle attack.

Audit:

Verify RHEL 9 does not accept router advertisements on all IPv6 interfaces by default, unless the system is a router.
Note: If IPv6 is disabled on the system, this requirement is Not Applicable.
Determine if router advertisements are not accepted by default by using the following command:

```
$ sudo sysctl net.ipv6.conf.default.accept_ra

net.ipv6.conf.default.accept_ra = 0
```

If the "accept_ra" value is not "0" and is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.
Check that the configuration files are present to enable this network parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F net.ipv6.conf.default.accept_ra | tail -1

net.ipv6.conf.default.accept_ra = 0
```

If "net.ipv6.conf.default.accept_ra" is not set to "0" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to not accept router advertisements on all IPv6 interfaces by default unless the system is a router.
Add or edit the following line in a single system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv6.conf.default.accept_ra = 0
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.201 RHEL-09-254035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent IPv6 Internet Control Message Protocol (ICMP) redirect messages from being accepted.

```
GROUP ID: V-257976
RULE ID: SV-257976r991589
```

Rationale:

ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.

Audit:

Verify RHEL 9 will not accept IPv6 ICMP redirect messages.
Note: If IPv6 is disabled on the system, this requirement is Not Applicable.
Check the value of the default "accept_redirects" variables with the following command:

```
$ sudo sysctl net.ipv6.conf.default.accept_redirects

net.ipv6.conf.default.accept_redirects = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.
Check that the configuration files are present to enable this network parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F net.ipv6.conf.default.accept_redirects | tail -1

net.ipv6.conf.default.accept_redirects = 0
```

If "net.ipv6.conf.default.accept_redirects" is not set to "0" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to prevent IPv6 ICMP redirect messages from being accepted.
Add or edit the following line in a single system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv6.conf.default.accept_redirects = 0
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.202 RHEL-09-254040 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not forward IPv6 source-routed packets by default.

```
GROUP ID: V-257977
RULE ID: SV-257977r991589
```

Rationale:

Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when forwarding is enabled and the system is functioning as a router.

Accepting source-routed packets in the IPv6 protocol has few legitimate uses. It must be disabled unless it is absolutely required.

Audit:

Verify RHEL 9 does not accept IPv6 source-routed packets by default.
Note: If IPv6 is disabled on the system, this requirement is Not Applicable.
Check the value of the accept source route variable with the following command:

```
$ sudo sysctl net.ipv6.conf.default.accept_source_route

net.ipv6.conf.default.accept_source_route = 0
```

If the returned line does not have a value of "0", a line is not returned, or the line is commented out, this is a finding.
Check that the configuration files are present to enable this network parameter.

```
$ sudo /usr/lib/systemd/systemd-sysctl --cat-config | egrep -v '^(#|;)' |
grep -F net.ipv6.conf.default.accept_source_route | tail -1

net.ipv6.conf.default.accept_source_route = 0
```

If "net.ipv6.conf.default.accept_source_route" is not set to "0" or is missing, this is a finding.

Remediation:

Configure RHEL 9 to not forward IPv6 source-routed packets by default.
Add or edit the following line in a single system configuration file, in the "/etc/sysctl.d/" directory:

```
net.ipv6.conf.default.accept_source_route = 0
```

Load settings from all system configuration files with the following command:

```
$ sudo sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.203 RHEL-09-255010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

All RHEL 9 networked systems must have SSH installed.

```
GROUP ID: V-257978
RULE ID: SV-257978r1045013
```

Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Audit:

Verify that RHEL 9 has the openssh-server package installed with the following command:

```
$ dnf list --installed openssh-server
```

Example output:

```
openssh-server.x86_64          8.7p1-8.el9
```

If the "openssh-server" package is not installed, this is a finding.

Remediation:

The openssh-server package can be installed with the following command:

```
$ sudo dnf install openssh-server
```

Additional Information:

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4 :: SC-8
- NIST SP 800-53 Revision 5 :: SC-8

CCI-002420 Maintain the confidentiality and/or integrity of information during preparation for transmission.

- NIST SP 800-53 Revision 4 :: SC-8 (2)
- NIST SP 800-53 Revision 5 :: SC-8 (2)

CCI-002421 Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4 :: SC-8 (1)
- NIST SP 800-53 Revision 5 :: SC-8 (1)

CCI-002422 Maintain the confidentiality and/or integrity of information during reception.

- NIST SP 800-53 Revision 4 :: SC-8 (2)
- NIST SP 800-53 Revision 5 :: SC-8 (2)

1.204 RHEL-09-255015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

All RHEL 9 networked systems must have and implement SSH to protect the confidentiality and integrity of transmitted and received information, as well as information during preparation for transmission.

```
GROUP ID: V-257979
RULE ID: SV-257979r958908
```

Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Audit:

Verify that "sshd" is active with the following command:

```
$ systemctl is-active sshd

active
```

If the "sshd" service is not active, this is a finding.

Remediation:

To enable the sshd service run the following command:

```
$ systemctl enable --now sshd
```

Additional Information:

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4 :: SC-8
- NIST SP 800-53 Revision 5 :: SC-8

CCI-002420 Maintain the confidentiality and/or integrity of information during preparation for transmission.

- NIST SP 800-53 Revision 4 :: SC-8 (2)
- NIST SP 800-53 Revision 5 :: SC-8 (2)

CCI-002421 Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4 :: SC-8 (1)
- NIST SP 800-53 Revision 5 :: SC-8 (1)

CCI-002422 Maintain the confidentiality and/or integrity of information during reception.

- NIST SP 800-53 Revision 4 :: SC-8 (2)
- NIST SP 800-53 Revision 5 :: SC-8 (2)

1.205 RHEL-09-255020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must have the openssh-clients package installed.

```
GROUP ID: V-257980
RULE ID: SV-257980r1045016
```

Rationale:

This package includes utilities to make encrypted connections and transfer files securely to SSH servers.

Audit:

Verify that RHEL 9 has the openssh-clients package installed with the following command:

```
$ dnf list --installed openssh-clients
```

Example output:

```
openssh-clients.x86_64          8.7p1-8.el9
```

If the "openssh-clients" package is not installed, this is a finding.

Remediation:

The openssh-clients package can be installed with the following command:

```
$ sudo dnf install openssh-clients
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.206 RHEL-09-255025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must display the Standard Mandatory DOD Notice and Consent Banner before granting local or remote access to the system via a SSH logon.

```
GROUP ID: V-257981
RULE ID: SV-257981r1045019
```

Rationale:

The warning message reinforces policy awareness during the logon process and facilitates possible legal action against attackers. Alternatively, systems whose ownership should not be obvious should ensure usage of a banner that does not provide easy attribution.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000228-GPOS-00088

Audit:

Verify that any SSH 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 currently being used with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*banner'

banner /etc/issue
```

If the line is commented out or if the file is missing, this is a finding.

Remediation:

Configure RHEL 9 to display the Standard Mandatory DOD Notice and Consent Banner before granting access to the system via ssh.
Edit the "etc/ssh/sshd_config" file or a file in "/etc/ssh/sshd_config.d" 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).
An example configuration line is:

```
Banner /etc/issue
```

Additional Information:

CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53 :: AC-8 a
- NIST SP 800-53 Revision 4 :: AC-8 a
- NIST SP 800-53 Revision 5 :: AC-8 a
- NIST SP 800-53A :: AC-8.1 (ii)

CCI-001384 For publicly accessible systems, display system use information with organization-defined conditions before granting further access to the publicly accessible system.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 1
- NIST SP 800-53 Revision 5 :: AC-8 c 1
- NIST SP 800-53A :: AC-8.2 (i)

CCI-001385 For publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2
- NIST SP 800-53A :: AC-8.2 (ii)

CCI-001386 For publicly accessible systems, displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2
- NIST SP 800-53A :: AC-8.2 (ii)

CCI-001387 For publicly accessible systems, displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2
- NIST SP 800-53A :: AC-8.2 (ii)

CCI-001388 For publicly accessible systems, includes a description of the authorized uses of the system.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 3
- NIST SP 800-53 Revision 5 :: AC-8 c 3
- NIST SP 800-53A :: AC-8.2 (iii)

1.207 RHEL-09-255030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must log SSH connection attempts and failures to the server.

```
GROUP ID: V-257982
RULE ID: SV-257982r1045021
```

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. "INFO" or "VERBOSE" 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.

Audit:

Verify that RHEL 9 logs SSH connection attempts and failures to the server.
Check what the SSH daemon's "LogLevel" option is set to with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*loglevel'

LogLevel VERBOSE
```

If a value of "VERBOSE" is not returned or the line is commented out or missing, this is a finding.

Remediation:

Configure RHEL 9 to log connection attempts add or modify the following line in "/etc/ssh/sshd_config" or in a file in "/etc/ssh/sshd_config.d".

```
LogLevel VERBOSE
```

Restart the SSH daemon for the settings to take effect:

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000067 Employ automated mechanisms to monitor remote access methods.

- NIST SP 800-53 :: AC-17 (1)
- NIST SP 800-53 Revision 4 :: AC-17 (1)
- NIST SP 800-53 Revision 5 :: AC-17 (1)
- NIST SP 800-53A :: AC-17 (1).1

1.208 RHEL-09-255035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 SSHD must accept public key authentication.

```
GROUP ID: V-257983
RULE ID: SV-257983r1045024
```

Rationale:

Without the use of multifactor authentication, the ease of access to privileged functions is greatly increased. Multifactor authentication requires using two or more factors to achieve authentication. A privileged account is defined as an information system account with authorizations of a privileged user. A DOD common access card (CAC) with DOD-approved PKI is an example of multifactor authentication.

Satisfies: SRG-OS-000105-GPOS-00052, SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000108-GPOS-00055

Audit:

Note: If the system administrator demonstrates the use of an approved alternate multifactor authentication method, this requirement is Not Applicable.
Verify that RHEL 9 SSH daemon accepts public key encryption with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*pubkeyauthentication'

PubkeyAuthentication yes
```

If "PubkeyAuthentication" is set to no, the line is commented out, or the line is missing, this is a finding.

Remediation:

To configure the system, add or modify the following line in "/etc/ssh/sshd_config" or in a file in "/etc/ssh/sshd_config.d".

```
PubkeyAuthentication yes
```

Restart the SSH daemon for the settings to take effect:

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000765 Implement multifactor authentication for network access to privileged accounts.

- NIST SP 800-53 :: IA-2 (1)
- NIST SP 800-53 Revision 4 :: IA-2 (1)
- NIST SP 800-53 Revision 5 :: IA-2 (1)
- NIST SP 800-53A :: IA-2 (1).1

CCI-000766 Implement multifactor authentication for network access to non-privileged accounts.

- NIST SP 800-53 :: IA-2 (2)
- NIST SP 800-53 Revision 4 :: IA-2 (2)
- NIST SP 800-53 Revision 5 :: IA-2 (2)
- NIST SP 800-53A :: IA-2 (2).1

CCI-000767 The information system implements multifactor authentication for local access to privileged accounts.

- NIST SP 800-53 :: IA-2 (3)
- NIST SP 800-53 Revision 4 :: IA-2 (3)
- NIST SP 800-53A :: IA-2 (3).1

CCI-000768 The information system implements multifactor authentication for local access to non-privileged accounts.

- NIST SP 800-53 :: IA-2 (4)
- NIST SP 800-53 Revision 4 :: IA-2 (4)
- NIST SP 800-53A :: IA-2 (4).1

1.209 RHEL-09-255040 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

RHEL 9 SSHD must not allow blank passwords.

```
GROUP ID: V-257984
RULE ID: SV-257984r1045026
```

Rationale:

If an account has an empty password, anyone could log on and run commands with the privileges of that account. Accounts with empty passwords should never be used in operational environments.

Satisfies: SRG-OS-000106-GPOS-00053, SRG-OS-000480-GPOS-00229, SRG-OS-000480-GPOS-00227

Audit:

Verify that RHEL 9 remote access using SSH prevents logging on with a blank password with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*permitemptypasswords'

PermitEmptyPasswords no
```

If the "PermitEmptyPasswords" keyword is set to "yes", is missing, or is commented out, this is a finding.

Remediation:

To configure the system to prevent SSH users from logging on with blank passwords edit the following line in "/etc/ssh/sshd_config" or in a file in "/etc/ssh/sshd_config.d":

```
PermitEmptyPasswords no
```

Restart the SSH daemon for the settings to take effect:

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000766 Implement multifactor authentication for network access to non-privileged accounts.

- NIST SP 800-53 :: IA-2 (2)
- NIST SP 800-53 Revision 4 :: IA-2 (2)
- NIST SP 800-53 Revision 5 :: IA-2 (2)
- NIST SP 800-53A :: IA-2 (2).1

1.210 RHEL-09-255045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not permit direct logons to the root account using remote access via SSH.

```
GROUP ID: V-257985
RULE ID: SV-257985r1069364
```

Rationale:

Even though the communications channel may be encrypted, an additional layer of security is gained by extending the policy of not logging directly on as root. In addition, logging in with a user-specific account provides individual accountability of actions performed on the system and also helps to minimize direct attack attempts on root's password.

Satisfies: SRG-OS-000109-GPOS-00056, SRG-OS-000480-GPOS-00227

Audit:

Verify RHEL 9 remote access using SSH prevents users from logging on directly as "root" with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*permitrootlogin'

PermitRootLogin no
```

If the "PermitRootLogin" keyword is set to any value other than "no", is missing, or is commented out, this is a finding.

Remediation:

To configure the system to prevent SSH users from logging on directly as root add or modify the following line in "/etc/ssh/sshd_config" or in a file in "/etc/ssh/sshd_config.d".

```
PermitRootLogin no
```

Restart the SSH daemon for the settings to take effect:

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-004045 Require users to be individually authenticated before granting access to the shared accounts or resources.

- NIST SP 800-53 Revision 5 :: IA-2 (5)

CCI-000770 The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

- NIST SP 800-53 :: IA-2 (5) (b)
- NIST SP 800-53 Revision 4 :: IA-2 (5)
- NIST SP 800-53A :: IA-2 (5).2 (ii)

1.211 RHEL-09-255050 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

RHEL 9 must enable the Pluggable Authentication Module (PAM) interface for SSHD.

```
GROUP ID: V-257986
RULE ID: SV-257986r1045030
```

Rationale:

When UsePAM is set to "yes", PAM runs through account and session types properly. This is important when restricted access to services based off of IP, time, or other factors of the account is needed. Additionally, this ensures users can inherit certain environment variables on login or disallow access to the server.

Audit:

Verify the RHEL 9 SSHD is configured to allow for the UsePAM interface with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*usepam'

UsePAM yes
```

If the "UsePAM" keyword is set to "no", is missing, or is commented out, this is a finding.

Remediation:

Configure the RHEL 9 SSHD to use the UsePAM interface by adding or modifying the following line in "/etc/ssh/sshd_config" or in a file in "/etc/ssh/sshd_config.d".

```
UsePAM yes
```

Restart the SSH daemon for the settings to take effect:

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000877 Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 :: MA-4 c
- NIST SP 800-53 Revision 4 :: MA-4 c
- NIST SP 800-53 Revision 5 :: MA-4 c
- NIST SP 800-53A :: MA-4.1 (iv)

1.212 RHEL-09-255055 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 SSH daemon must be configured to use system-wide crypto policies

```
GROUP ID: V-257987
RULE ID: SV-257987r1014852
```

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

Audit:

Verify that systemwide crypto policies are in effect with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*include'

/etc/ssh/sshd_config:Include /etc/ssh/sshd_config.d/*.conf
/etc/ssh/sshd_config.d/50-redhat.conf:Include /etc/crypto-policies/back-
ends/opensshserver.config
```

If "Include /etc/ssh/sshd_config.d/*.conf" or "Include /etc/crypto-policies/back-ends/opensshserver.config" are not included in the system sshd config this is a finding. Additionally, if the file /etc/ssh/sshd_config.d/50-redhat.conf is missing, this is a finding.

Remediation:

Configure the RHEL 9 SSH daemon to use system-wide crypto policies by running the following commands:

```
$ sudo dnf reinstall openssh-server
```

Additional Information:

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53 :: AC-17 (2)
- NIST SP 800-53 Revision 4 :: AC-17 (2)
- NIST SP 800-53 Revision 5 :: AC-17 (2)
- NIST SP 800-53A :: AC-17 (2).1

1.213 RHEL-09-255060 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must implement DOD-approved encryption ciphers to protect the confidentiality of SSH connections.

```
GROUP ID: V-257988
RULE ID: SV-257988r1051234
```

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

RHEL 9 incorporates systemwide crypto policies by default. The SSH configuration file has no effect on the ciphers, MACs, or algorithms unless specifically defined in the /etc/sysconfig/sshd file. The employed algorithms can be viewed in the /etc/crypto-policies/back-ends/opensshserver.config file.

Audit:

Verify that RHEL 9 implements DOD-approved encryption ciphers for SSH connections. Verify that the SSH configuration files include the path to the systemwide policy with the following command:

```
$ sudo grep -R Include /etc/ssh/sshd_config  /etc/ssh/sshd_config.d/

/etc/ssh/sshd_config:Include /etc/ssh/sshd_config.d/*.conf
/etc/ssh/sshd_config.d/50-redhat.conf:Include /etc/crypto-policies/back-
ends/opensshserver.config
```

If "Include /etc/ssh/sshd_config.d/*.conf" or "Include /etc/crypto-policies/back-ends/opensshserver.config" are not included in the system sshd config or if the file "/etc/ssh/sshd_config.d/50-redhat.conf" is missing, this is a finding.

Remediation:

Configure the RHEL 9 SSH daemon to use systemwide crypto policies.
Reinstall OpenSSH client package contents with the following command:

```
$ sudo dnf -y reinstall openssh
```

Additional Information:

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53 :: AC-17 (2)
- NIST SP 800-53 Revision 4 :: AC-17 (2)
- NIST SP 800-53 Revision 5 :: AC-17 (2)
- NIST SP 800-53A :: AC-17 (2).1

1.214 RHEL-09-255064 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The RHEL 9 SSH client must be configured to use only DOD-approved encryption ciphers employing FIPS 140-3 validated cryptographic hash algorithms to protect the confidentiality of SSH client connections.

```
GROUP ID: V-270177
RULE ID: SV-270177r1051237
```

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography, enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

RHEL 9 incorporates systemwide crypto policies by default. The SSH configuration file has no effect on the ciphers, MACs, or algorithms unless specifically defined in the /etc/sysconfig/sshd file. The employed algorithms can be viewed in the /etc/crypto-policies/back-ends/openssh.config file.

Audit:

Verify the SSH client is configured to use only ciphers employing FIPS 140-3 approved algorithms.
To verify the ciphers in the systemwide SSH configuration file, use the following command:

```
$ grep -i Ciphers /etc/crypto-policies/back-ends/openssh.config

Ciphers aes256-gcm@openssh.com,aes256-ctr,aes128-gcm@openssh.com,aes128-ctr
```

If the cipher entries in the "openssh.config" file have any ciphers other than "aes256-gcm@openssh.com,aes256-ctr,aes128-gcm@openssh.com,aes128-ctr", or they are missing or commented out, this is a finding.

Remediation:

Configure the SSH client to use only ciphers employing FIPS 140-3 approved algorithms.
Reinstall crypto-policies with the following command:

```
$ sudo dnf -y reinstall crypto-policies
```

Set the crypto-policy to FIPS with the following command:

```
$ sudo update-crypto-policies --set FIPS

Setting system policy to FIPS
```

Note: Systemwide crypto policies are applied on application startup. It is recommended to restart the system for the change of policies to fully take place.

Additional Information:

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53 :: AC-17 (2)
- NIST SP 800-53 Revision 4 :: AC-17 (2)
- NIST SP 800-53 Revision 5 :: AC-17 (2)
- NIST SP 800-53A :: AC-17 (2).1

1.215 RHEL-09-255065 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The RHEL 9 SSH server must be configured to use only DOD-approved encryption ciphers employing FIPS 140-3 validated cryptographic hash algorithms to protect the confidentiality of SSH server connections.

```
GROUP ID: V-257989
RULE ID: SV-257989r1051240
```

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

RHEL 9 incorporates systemwide crypto policies by default. The SSH configuration file has no effect on the ciphers, MACs, or algorithms unless specifically defined in the /etc/sysconfig/sshd file. The employed algorithms can be viewed in the /etc/crypto-policies/back-ends/opensshserver.config file.

Audit:

Verify the SSH server is configured to use only ciphers employing FIPS 140-3 approved algorithms.
To verify the ciphers in the systemwide SSH configuration file, use the following command:

```
$ sudo grep -i Ciphers /etc/crypto-policies/back-ends/opensshserver.config
Ciphers aes256-gcm@openssh.com,aes256-ctr,aes128-gcm@openssh.com,aes128-ctr
```

If the cipher entries in the "opensshserver.config" file have any ciphers other than "aes256-gcm@openssh.com,aes256-ctr,aes128-gcm@openssh.com,aes128-ctr", or they are missing or commented out, this is a finding.

Remediation:

Configure the RHEL 9 SSH server to use only ciphers employing FIPS 140-3 approved algorithms.
Reinstall crypto-policies with the following command:

```
$ sudo dnf -y reinstall crypto-policies
```

Set the crypto-policy to FIPS with the following command:

```
$ sudo update-crypto-policies --set FIPS

Setting system policy to FIPS
```

Note: Systemwide crypto policies are applied on application startup. It is recommended to restart the system for the change of policies to fully take place.

Additional Information:

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53 :: AC-17 (2)
- NIST SP 800-53 Revision 4 :: AC-17 (2)
- NIST SP 800-53 Revision 5 :: AC-17 (2)
- NIST SP 800-53A :: AC-17 (2).1

1.216 RHEL-09-255070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The RHEL 9 SSH client must be configured to use only DOD-approved Message Authentication Codes (MACs) employing FIPS 140-3 validated cryptographic hash algorithms to protect the confidentiality of SSH client connections.

```
GROUP ID: V-270178
RULE ID: SV-270178r1051243
```

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography, enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

RHEL 9 incorporates systemwide crypto policies by default. The SSH configuration file has no effect on the ciphers, MACs, or algorithms unless specifically defined in the /etc/sysconfig/sshd file. The employed algorithms can be viewed in the /etc/crypto-policies/back-ends/openssh.config file.

Audit:

Verify the SSH client is configured to use only MACs employing FIPS 140-3 approved algorithms.
To verify the MACs in the systemwide SSH configuration file, use the following command:

```
$ grep -i MACs /etc/crypto-policies/back-ends/openssh.config

MACs hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-
256,hmac-sha2-512
```

If the MACs entries in the "openssh.config" file have any hashes other than "hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512", or they are missing or commented out, this is a finding.

Remediation:

Configure the SSH client to use only MACs employing FIPS 140-3 approved algorithms. Reinstall crypto-policies with the following command:

```
$ sudo dnf -y reinstall crypto-policies
```

Set the crypto-policy to FIPS with the following command:

```
$ sudo update-crypto-policies --set FIPS

Setting system policy to FIPS
```

Note: Systemwide crypto policies are applied on application startup. It is recommended to restart the system for the change of policies to fully take place.

Additional Information:

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53 :: AC-17 (2)
- NIST SP 800-53 Revision 4 :: AC-17 (2)
- NIST SP 800-53 Revision 5 :: AC-17 (2)
- NIST SP 800-53A :: AC-17 (2).1

1.217 RHEL-09-255075 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The RHEL 9 SSH server must be configured to use only Message Authentication Codes (MACs) employing FIPS 140-3 validated cryptographic hash algorithms to protect the confidentiality of SSH server connections.

```
GROUP ID: V-257991
RULE ID: SV-257991r1051246
```

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

RHEL 9 incorporates systemwide crypto policies by default. The SSH configuration file has no effect on the ciphers, MACs, or algorithms unless specifically defined in the /etc/sysconfig/sshd file. The employed algorithms can be viewed in the /etc/crypto-policies/back-ends/opensshserver.config file.

Audit:

Verify the SSH server is configured to use only MACs employing FIPS 140-3 approved algorithms.
To verify the MACs in the systemwide SSH configuration file, use the following command:

```
$ sudo grep -i MACs /etc/crypto-policies/back-ends/opensshserver.config

MACs hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-
256,hmac-sha2-512
```

If the MACs entries in the "opensshserver.config" file have any hashes other than "hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512", or they are missing or commented out, this is a finding.

Remediation:

Configure the RHEL 9 SSH server to use only MACs employing FIPS 140-3 approved algorithms.
Reinstall crypto-policies with the following command:

```
$ sudo dnf -y reinstall crypto-policies
```

Set the crypto-policy to FIPS with the following command:

```
$ sudo update-crypto-policies --set FIPS

Setting system policy to FIPS
```

Note: Systemwide crypto policies are applied on application startup. It is recommended to restart the system for the change of policies to fully take place.

Additional Information:

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53 :: AC-17 (2)
- NIST SP 800-53 Revision 4 :: AC-17 (2)
- NIST SP 800-53 Revision 5 :: AC-17 (2)
- NIST SP 800-53A :: AC-17 (2).1

1.218 RHEL-09-255080 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not allow a noncertificate trusted host SSH logon to the system.

```
GROUP ID: V-257992
RULE ID: SV-257992r1045047
```

Rationale:

SSH trust relationships mean a compromise on one host can allow an attacker to move trivially to other hosts.

Audit:

Verify the operating system does not allow a noncertificate trusted host SSH logon to the system with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*hostbasedauthentication'

HostbasedAuthentication no
```

If the "HostbasedAuthentication" keyword is not set to "no", is missing, or is commented out, this is a finding.
If the required value is not set, this is a finding.

Remediation:

To configure RHEL 9 to not allow a noncertificate trusted host SSH logon to the system, add or modify the following line in "/etc/ssh/sshd_config" or in a file in "/etc/ssh/sshd_config.d".

```
HostbasedAuthentication no
```

Restart the SSH daemon for the settings to take effect:

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.219 RHEL-09-255085 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not allow users to override SSH environment variables.

```
GROUP ID: V-257993
RULE ID: SV-257993r1045049
```

Rationale:

SSH environment options potentially allow users to bypass access restriction in some configurations.

Audit:

Verify that unattended or automatic logon via SSH is disabled with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*permituserenvironment'

PermitUserEnvironment no
```

If "PermitUserEnvironment" is set to "yes", is missing completely, or is commented out, this is a finding.
If the required value is not set, this is a finding.

Remediation:

Configure the RHEL 9 SSH daemon to not allow unattended or automatic logon to the system by editing the following line in the "/etc/ssh/sshd_config" or in a file in "/etc/ssh/sshd_config.d":

```
PermitUserEnvironment no
```

Restart the SSH daemon for the setting to take effect:

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.220 RHEL-09-255090 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must force a frequent session key renegotiation for SSH connections to the server.

```
GROUP ID: V-257994
RULE ID: SV-257994r1045051
```

Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Session key regeneration limits the chances of a session key becoming compromised.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000033-GPOS-00014, SRG-OS-000424-GPOS-00188

Audit:

Verify the SSH server is configured to force frequent session key renegotiation with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*rekeylimit'

RekeyLimit 1G 1h
```

If "RekeyLimit" does not have a maximum data amount and maximum time defined, is missing, or is commented out, this is a finding.

Remediation:

Configure RHEL 9 to force a frequent session key renegotiation for SSH connections to the server by adding or modifying the following line in the "/etc/ssh/sshd_config" or in a file in "/etc/ssh/sshd_config.d":

```
RekeyLimit 1G 1h
```

Restart the SSH daemon for the settings to take effect.

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53 :: AC-17 (2)
- NIST SP 800-53 Revision 4 :: AC-17 (2)
- NIST SP 800-53 Revision 5 :: AC-17 (2)
- NIST SP 800-53A :: AC-17 (2).1

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4 :: SC-8
- NIST SP 800-53 Revision 5 :: SC-8

CCI-002421 Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4 :: SC-8 (1)
- NIST SP 800-53 Revision 5 :: SC-8 (1)

1.221 RHEL-09-255095 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must be configured so that all network connections associated with SSH traffic terminate after becoming unresponsive.

```
GROUP ID: V-257995
RULE ID: SV-257995r1045053
```

Rationale:

Terminating an unresponsive SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, deallocating associated TCP/IP address/port pairs at the operating system level and deallocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean the operating system terminates all sessions or network access; it only ends the unresponsive session and releases the resources associated with that session.

RHEL 9 utilizes /etc/ssh/sshd_config for configurations of OpenSSH. Within the sshd_config, the product of the values of "ClientAliveInterval" and "ClientAliveCountMax" are used to establish the inactivity threshold. The "ClientAliveInterval" is a timeout interval in seconds, after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. The "ClientAliveCountMax" is the number of client alive messages that may be sent without sshd receiving any messages back from the client. If this threshold is met, sshd will disconnect the client. For more information on these settings and others, refer to the sshd_config man pages.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109

Audit:

Verify the "ClientAliveCountMax" is set to "1" by performing the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*clientalivecountmax'

ClientAliveCountMax 1
```

If "ClientAliveCountMax" does not exist, is not set to a value of "1" in "/etc/ssh/sshd_config", or is commented out, this is a finding.

Remediation:

Note: This setting must be applied in conjunction with RHEL-09-255100 to function correctly.
Configure the SSH server to terminate a user session automatically after the SSH client has become unresponsive.
Modify or append the following lines in the "/etc/ssh/sshd_config" or in a file in "/etc/ssh/sshd_config.d":

```
ClientAliveCountMax 1
```

For the changes to take effect, the SSH daemon must be restarted.

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53 :: SC-10
- NIST SP 800-53 Revision 4 :: SC-10
- NIST SP 800-53 Revision 5 :: SC-10
- NIST SP 800-53A :: SC-10.1 (ii)

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4 :: AC-12
- NIST SP 800-53 Revision 5 :: AC-12

1.222 RHEL-09-255100 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must be configured so that all network connections associated with SSH traffic are terminated after 10 minutes of becoming unresponsive.

```
GROUP ID: V-257996
RULE ID: SV-257996r1045055
```

Rationale:

Terminating an unresponsive SSH session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle SSH session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, deallocating associated TCP/IP address/port pairs at the operating system level and deallocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean the operating system terminates all sessions or network access; it only ends the unresponsive session and releases the resources associated with that session.

RHEL 9 utilizes /etc/ssh/sshd_config for configurations of OpenSSH. Within the sshd_config, the product of the values of "ClientAliveInterval" and "ClientAliveCountMax" are used to establish the inactivity threshold. The "ClientAliveInterval" is a timeout interval in seconds, after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. The "ClientAliveCountMax" is the number of client alive messages that may be sent without sshd receiving any messages back from the client. If this threshold is met, sshd will disconnect the client. For more information on these settings and others, refer to the sshd_config man pages.

Satisfies: SRG-OS-000126-GPOS-00066, SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109, SRG-OS-000395-GPOS-00175

Audit:

Verify the "ClientAliveInterval" variable is set to a value of "600" or less by performing the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*clientaliveinterval'

ClientAliveInterval 600
```

If "ClientAliveInterval" does not exist, does not have a value of "600" or less in "/etc/ssh/sshd_config", or is commented out, this is a finding.

Remediation:

Note: This setting must be applied in conjunction with RHEL-09-255095 to function correctly.
Configure the SSH server to terminate a user session automatically after the SSH client has been unresponsive for 10 minutes.
Modify or append the following lines in the "/etc/ssh/sshd_config" or in a file in "/etc/ssh/sshd_config.d":

```
ClientAliveInterval 600
```

For the changes to take effect, the SSH daemon must be restarted.

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53 :: SC-10
- NIST SP 800-53 Revision 4 :: SC-10
- NIST SP 800-53 Revision 5 :: SC-10
- NIST SP 800-53A :: SC-10.1 (ii)

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4 :: AC-12
- NIST SP 800-53 Revision 5 :: AC-12

CCI-002891 Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (7)
- NIST SP 800-53 Revision 5 :: MA-4 (7)

1.223 RHEL-09-255105 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 SSH server configuration file must be group-owned by root.

```
GROUP ID: V-257997
RULE ID: SV-257997r1069370
```

Rationale:

Service configuration files enable or disable features of their respective services, which if configured incorrectly, can lead to insecure and vulnerable configurations. Therefore, service configuration files must be owned by the correct group to prevent unauthorized changes.

Audit:

Verify the group ownership of the "/etc/ssh/sshd_config" file and the contents of "/etc/ssh/sshd_config.d" with the following command:

```
$ sudo find /etc/ssh/sshd_config /etc/ssh/sshd_config.d -exec stat -c "%G %n"
{} \;

root /etc/ssh/sshd_config
root /etc/ssh/sshd_config.d
root /etc/ssh/sshd_config.d/50-cloud-init.conf
root /etc/ssh/sshd_config.d/50-redhat.conf
```

If the "/etc/ssh/sshd_config" file or "/etc/ssh/sshd_config.d" or any files in the sshd_config.d directory do not have a group owner of "root", this is a finding.

Remediation:

Configure the "/etc/ssh/sshd_config" file and the contents of "/etc/ssh/sshd_config.d" to be group-owned by root with the following command:

```
$ sudo chgrp root /etc/ssh/sshd_config /etc/ssh/sshd_config.d
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.224 RHEL-09-255110 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 SSH server configuration file must be owned by root.

```
GROUP ID: V-257998
RULE ID: SV-257998r1082181
```

Rationale:

Service configuration files enable or disable features of their respective services, which if configured incorrectly, can lead to insecure and vulnerable configurations. Therefore, service configuration files must be owned by the correct group to prevent unauthorized changes.

Audit:

Verify the ownership of the "/etc/ssh/sshd_config" file and the contents of "/etc/ssh/sshd_config.d" with the following command:

```
$ sudo find /etc/ssh/sshd_config /etc/ssh/sshd_config.d -exec stat -c "%U %n"
{} \;

root /etc/ssh/sshd_config
root /etc/ssh/sshd_config.d
root /etc/ssh/sshd_config.d/50-cloud-init.conf
root /etc/ssh/sshd_config.d/50-redhat.conf
```

If the "/etc/ssh/sshd_config" file or "/etc/ssh/sshd_config.d" or any files in the "sshd_config.d" directory do not have an owner of "root", this is a finding.

Remediation:

Configure the "/etc/ssh/sshd_config" file and the contents of "/etc/ssh/sshd_config.d" to be owned by root with the following command:

```
$ sudo chown -R root /etc/ssh/sshd_config /etc/ssh/sshd_config.d
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.225 RHEL-09-255115 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 SSH server configuration files' permissions must not be modified.

```
GROUP ID: V-257999
RULE ID: SV-257999r1082182
```

Rationale:

Service configuration files enable or disable features of their respective services, that if configured incorrectly, can lead to insecure and vulnerable configurations. Therefore, service configuration files must have correct permissions (owner, group owner, mode) to prevent unauthorized changes.

Audit:

Verify the permissions of the "/etc/ssh/sshd_config" file with the following command:

```
$ sudo rpm --verify openssh-server
```

If the command returns any output, this is a finding.

Remediation:

Run the following commands to restore the correct permissions of OpenSSH server configuration files:

```
$ sudo dnf reinstall -y openssh-server
$ rpm --setugids openssh-server
$ rpm --setperms openssh-server
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.226 RHEL-09-255120 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 SSH private host key files must have mode 0640 or less permissive.

```
GROUP ID: V-258000
RULE ID: SV-258000r1045063
```

Rationale:

If an unauthorized user obtains the private SSH host key file, the host could be impersonated.

Audit:

Verify the SSH private host key files have a mode of "0640" or less permissive with the following command:

```
$ stat -c "%a %n" /etc/ssh/*_key

640 /etc/ssh/ssh_host_dsa_key
640 /etc/ssh/ssh_host_ecdsa_key
640 /etc/ssh/ssh_host_ed25519_key
640 /etc/ssh/ssh_host_rsa_key
```

If any private host key file has a mode more permissive than "0640", this is a finding.

Remediation:

Configure the mode of SSH private host key files under "/etc/ssh" to "0640" with the following command:

```
$ sudo chmod 0640 /etc/ssh/ssh_host*key
```

Restart the SSH daemon for the changes to take effect:

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.227 RHEL-09-255125 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 SSH public host key files must have mode 0644 or less permissive.

```
GROUP ID: V-258001
RULE ID: SV-258001r991589
```

Rationale:

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

Audit:

Verify the SSH public host key files have a mode of "0644" or less permissive with the following command:
Note: SSH public key files may be found in other directories on the system depending on the installation.

```
$ sudo stat -c "%a %n" /etc/ssh/*.pub

644 /etc/ssh/ssh_host_dsa_key.pub
644 /etc/ssh/ssh_host_ecdsa_key.pub
644 /etc/ssh/ssh_host_ed25519_key.pub
644 /etc/ssh/ssh_host_rsa_key.pub
```

If any key.pub file has a mode more permissive than "0644", this is a finding.

Remediation:

Change the mode of public host key files under "/etc/ssh" to "0644" with the following command:

```
$ sudo chmod 0644 /etc/ssh/*key.pub
```

Restart the SSH daemon for the changes to take effect:

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.228 RHEL-09-255130 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 SSH daemon must not allow compression or must only allow compression after successful authentication.

```
GROUP ID: V-258002
RULE ID: SV-258002r991589
```

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 with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*compression'

Compression delayed
```

If the "Compression" keyword is set to "yes", is missing, or the returned line is commented out, this is a finding.

Remediation:

Configure the SSH daemon to not allow compression.
Uncomment the "Compression" keyword in "/etc/ssh/sshd_config" on the system and set the value to "delayed" or "no":

```
Compression no
```

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

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.229 RHEL-09-255135 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 SSH daemon must not allow GSSAPI authentication.

```
GROUP ID: V-258003
RULE ID: SV-258003r1045065
```

Rationale:

Generic Security Service Application Program Interface (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.

Satisfies: SRG-OS-000364-GPOS-00151, SRG-OS-000480-GPOS-00227

Audit:

Verify the SSH daemon does not allow GSSAPI authentication with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*gssapiauthentication'

GSSAPIAuthentication no
```

If the value is returned as "yes", the returned line is commented out, no output is returned, and the use of GSSAPI authentication has not been documented with the information system security officer (ISSO), this is a finding.
If the required value is not set, this is a finding.

Remediation:

Configure the SSH daemon to not allow GSSAPI authentication.
Add or uncomment the following line to "/etc/ssh/sshd_config" or to a file in "/etc/ssh/sshd_config.d" and set the value to "no":

```
GSSAPIAuthentication no
```

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

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-001813 Enforce access restrictions using organization-defined mechanisms.

- NIST SP 800-53 Revision 4 :: CM-5 (1)
- NIST SP 800-53 Revision 5 :: CM-5 (1) (a)

1.230 RHEL-09-255140 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 SSH daemon must not allow Kerberos authentication.

```
GROUP ID: V-258004
RULE ID: SV-258004r1045067
```

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 implementations may be subject to exploitation.

Satisfies: SRG-OS-000364-GPOS-00151, SRG-OS-000480-GPOS-00227

Audit:

Verify the SSH daemon does not allow Kerberos authentication with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*kerberosauthentication'

KerberosAuthentication no
```

If the value is returned as "yes", the returned line is commented out, no output is returned, and the use of Kerberos authentication has not been documented with the information system security officer (ISSO), this is a finding.

Remediation:

Configure the SSH daemon to not allow Kerberos authentication.
Add the following line in "/etc/ssh/sshd_config" or to a file in "/etc/ssh/sshd_config.d", or uncomment the line and set the value to "no":

```
KerberosAuthentication no
```

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

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-001813 Enforce access restrictions using organization-defined mechanisms.

- NIST SP 800-53 Revision 4 :: CM-5 (1)
- NIST SP 800-53 Revision 5 :: CM-5 (1) (a)

1.231 RHEL-09-255145 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 SSH daemon must not allow rhosts authentication.

```
GROUP ID: V-258005
RULE ID: SV-258005r1045069
```

Rationale:

SSH trust relationships mean a compromise on one host can allow an attacker to move trivially to other hosts.

Audit:

Verify the SSH daemon does not allow rhosts authentication with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*ignorerhosts'

IgnoreRhosts yes
```

If the value is returned as "no", the returned line is commented out, or no output is returned, this is a finding.

Remediation:

Configure the SSH daemon to not allow rhosts authentication.
Add the following line to "/etc/ssh/sshd_config" or to a file in "/etc/ssh/sshd_config.d", or uncomment the line and set the value to "yes":

```
IgnoreRhosts yes
```

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

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.232 RHEL-09-255150 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 SSH daemon must not allow known hosts authentication.

```
GROUP ID: V-258006
RULE ID: SV-258006r1045071
```

Rationale:

Configuring the IgnoreUserKnownHosts setting for the SSH daemon provides additional assurance that remote login via SSH will require a password, even in the event of misconfiguration elsewhere.

Audit:

Verify the SSH daemon does not allow known hosts authentication with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*ignoreuserknownhosts'

IgnoreUserKnownHosts yes
```

If the value is returned as "no", the returned line is commented out, or no output is returned, this is a finding.

Remediation:

Configure the SSH daemon to not allow known hosts authentication.
Add the following line to "/etc/ssh/sshd_config" or to a file in "/etc/ssh/sshd_config.d", or uncomment the line and set the value to "yes":

```
IgnoreUserKnownHosts yes
```

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

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.233 RHEL-09-255155 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 SSH daemon must disable remote X connections for interactive users.

```
GROUP ID: V-258007
RULE ID: SV-258007r1045073
```

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 does not allow X11Forwarding with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*x11forwarding'

X11forwarding no
```

If the value is returned as "yes", the returned line is commented out, or no output is returned, and X11 forwarding is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Configure the SSH daemon to not allow X11 forwarding.
Add the following line to "/etc/ssh/sshd_config" or to a file in "/etc/ssh/sshd_config.d", or uncomment the line and set the value to "no":

```
X11forwarding no
```

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

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.234 RHEL-09-255160 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 SSH daemon must perform strict mode checking of home directory configuration files.

```
GROUP ID: V-258008
RULE ID: SV-258008r1045075
```

Rationale:

If other users have access to modify user-specific SSH configuration files, they may be able to log into the system as another user.

Audit:

Verify the SSH daemon performs strict mode checking of home directory configuration files with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*strictmodes'

StrictModes yes
```

If the "StrictModes" keyword is set to "no", the returned line is commented out, or no output is returned, this is a finding.

Remediation:

Configure the SSH daemon to perform strict mode checking of home directory configuration files.
Add the following line to "/etc/ssh/sshd_config" or to a file in "/etc/ssh/sshd_config.d", or uncomment the line and set the value to "yes":

```
StrictModes yes
```

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

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.235 RHEL-09-255165 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 SSH daemon must display the date and time of the last successful account logon upon an SSH logon.

```
GROUP ID: V-258009
RULE ID: SV-258009r1045077
```

Rationale:

Providing users feedback on when account accesses last occurred facilitates user recognition and reporting of unauthorized account use.

Audit:

Verify the SSH daemon provides users with feedback on when account accesses last occurred with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*printlastlog'

PrintLastLog yes
```

If the "PrintLastLog" keyword is set to "no", the returned line is commented out, or no output is returned, this is a finding.

Remediation:

Configure the SSH daemon to provide users with feedback on when account accesses last occurred.
Add the following line to "/etc/ssh/sshd_config" or to a file in "/etc/ssh/sshd_config.d", or uncomment the line and set the value to "yes":

```
PrintLastLog yes
```

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

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.236 RHEL-09-255175 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 SSH daemon must prevent remote hosts from connecting to the proxy display.

```
GROUP ID: V-258011
RULE ID: SV-258011r1045079
```

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 with the following command:

```
$ sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' |
tr '\n' ' ' | xargs sudo grep -iH '^\s*x11uselocalhost'

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.
Add the following line to "/etc/ssh/sshd_config" or to a file in "/etc/ssh/sshd_config.d", or uncomment the line and set the value to "yes":

```
X11UseLocalhost yes
```

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

```
$ sudo systemctl restart sshd.service
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.237 RHEL-09-271010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must display the Standard Mandatory DOD Notice and Consent Banner before granting local or remote access to the system via a graphical user logon.

```
GROUP ID: V-258012
RULE ID: SV-258012r1014855
```

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.

For U.S. Government systems, system use notifications are required only for access via login interfaces with human users and are not required when such human interfaces do not exist.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000228-GPOS-00088

Audit:

Verify RHEL 9 displays the Standard Mandatory DOD Notice and Consent Banner before granting access to the operating system via a graphical user logon.
Note: This requirement assumes the use of the RHEL 9 default graphical user interface, the GNOME desktop environment. If the system does not have any graphical user interface installed, this requirement is Not Applicable.
Determine if the operating system displays a banner at the logon screen with the following command:

```
$ gsettings get org.gnome.login-screen banner-message-enable

true
```

If the result is "false", this is a finding.

Remediation:

Configure RHEL 9 to display the Standard Mandatory DOD Notice and Consent Banner before granting access to the system via a graphical user logon.
Create a database to contain the system-wide graphical user logon settings (if it does not already exist) with the following command:

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

Add the following lines 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
```

Run the following command to update the database:

```
$ sudo dconf update
```

Additional Information:

CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53 :: AC-8 a
- NIST SP 800-53 Revision 4 :: AC-8 a
- NIST SP 800-53 Revision 5 :: AC-8 a
- NIST SP 800-53A :: AC-8.1 (ii)

CCI-001384 For publicly accessible systems, display system use information with organization-defined conditions before granting further access to the publicly accessible system.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 1
- NIST SP 800-53 Revision 5 :: AC-8 c 1
- NIST SP 800-53A :: AC-8.2 (i)

CCI-001385 For publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2
- NIST SP 800-53A :: AC-8.2 (ii)

CCI-001386 For publicly accessible systems, displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2
- NIST SP 800-53A :: AC-8.2 (ii)

CCI-001387 For publicly accessible systems, displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2
- NIST SP 800-53A :: AC-8.2 (ii)

CCI-001388 For publicly accessible systems, includes a description of the authorized uses of the system.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 3
- NIST SP 800-53 Revision 5 :: AC-8 c 3
- NIST SP 800-53A :: AC-8.2 (iii)

1.238 RHEL-09-271015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent a user from overriding the banner-message-enable setting for the graphical user interface.

```
GROUP ID: V-258013
RULE ID: SV-258013r1045082
```

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.

For U.S. Government systems, system use notifications are required only for access via login interfaces with human users and are not required when such human interfaces do not exist.

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000228-GPOS-00088

Audit:

Note: This requirement assumes the use of the RHEL 9 default graphical user interface, the GNOME desktop environment. If the system does not have any graphical user interface installed, this requirement is Not Applicable.
Verify RHEL 9 prevents a user from overriding settings for graphical user interfaces. Determine if the org.gnome.login-screen banner-message-enable key is writable with the following command:

```
$ gsettings writable org.gnome.login-screen banner-message-enable

false
```

If "banner-message-enable" is writable or the result is "true", this is a finding.

Remediation:

Configure RHEL 9 to prevent a user from overriding the banner setting for graphical user interfaces.
Create a database to contain the systemwide graphical user logon settings (if it does not already exist) with the following command:

```
$ sudo touch /etc/dconf/db/local.d/locks/session
```

Add the following setting to prevent nonprivileged users from modifying it:

```
/org/gnome/login-screen/banner-message-enable
```

Run the following command to update the database:

```
$ sudo dconf update
```

Additional Information:

CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53 :: AC-8 a
- NIST SP 800-53 Revision 4 :: AC-8 a
- NIST SP 800-53 Revision 5 :: AC-8 a
- NIST SP 800-53A :: AC-8.1 (ii)

CCI-001384 For publicly accessible systems, display system use information with organization-defined conditions before granting further access to the publicly accessible system.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 1
- NIST SP 800-53 Revision 5 :: AC-8 c 1
- NIST SP 800-53A :: AC-8.2 (i)

CCI-001385 For publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2
- NIST SP 800-53A :: AC-8.2 (ii)

CCI-001386 For publicly accessible systems, displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2
- NIST SP 800-53A :: AC-8.2 (ii)

CCI-001387 For publicly accessible systems, displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 2
- NIST SP 800-53 Revision 5 :: AC-8 c 2
- NIST SP 800-53A :: AC-8.2 (ii)

CCI-001388 For publicly accessible systems, includes a description of the authorized uses of the system.

- NIST SP 800-53 :: AC-8 c
- NIST SP 800-53 Revision 4 :: AC-8 c 3
- NIST SP 800-53 Revision 5 :: AC-8 c 3
- NIST SP 800-53A :: AC-8.2 (iii)

1.239 RHEL-09-271020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must disable the graphical user interface automount function unless required.

```
GROUP ID: V-258014
RULE ID: SV-258014r1045084
```

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: This requirement assumes the use of the RHEL 9 default graphical user interface, the GNOME desktop environment. If the system does not have any graphical user interface installed, this requirement is Not Applicable.
Verify RHEL 9 disables the graphical user interface automount function with the following command:

```
$ gsettings get org.gnome.desktop.media-handling automount-open

false
```

If "automount-open" is set to "true", and is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Configure the GNOME desktop to disable automated mounting of removable media.
The dconf settings can be edited in the /etc/dconf/db/* location.
Update the [org/gnome/desktop/media-handling] section of the "/etc/dconf/db/local.d/00-security-settings" database file and add or update the following lines:

```
[org/gnome/desktop/media-handling]
automount-open=false
```

Then update the dconf system databases:

```
$ sudo dconf update
```

Additional Information:

CCI-000778 Uniquely identify organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 :: IA-3
- NIST SP 800-53 Revision 4 :: IA-3
- NIST SP 800-53 Revision 5 :: IA-3
- NIST SP 800-53A :: IA-3.1 (ii)

CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4 :: IA-3
- NIST SP 800-53 Revision 5 :: IA-3

1.240 RHEL-09-271025 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent a user from overriding the disabling of the graphical user interface automount function.

```
GROUP ID: V-258015
RULE ID: SV-258015r1045086
```

Rationale:

A nonprivileged account is any operating system account with authorizations of a nonprivileged user.

Satisfies: SRG-OS-000114-GPOS-00059, SRG-OS-000378-GPOS-00163, SRG-OS-000480-GPOS-00227

Audit:

Note: This requirement assumes the use of the RHEL 9 default graphical user interface, the GNOME desktop environment. If the system does not have any graphical user interface installed, this requirement is Not Applicable.
Verify RHEL 9 disables the ability of the user to override the graphical user interface automount setting.
Determine which profile the system database is using with the following command:

```
$ sudo grep system-db /etc/dconf/profile/user

system-db:local
```

Check that the automount setting is locked from nonprivileged user modification with the following command:
Note: The example below is using the database "local" for the system, so the path is "/etc/dconf/db/local.d". This path must be modified if a database other than "local" is being used.

```
$ grep 'automount-open' /etc/dconf/db/local.d/locks/*

/org/gnome/desktop/media-handling/automount-open
```

If the command does not return at least the example result, this is a finding.

Remediation:

Configure the GNOME desktop to not allow a user to change the setting that disables automated mounting of removable media.
Add the following line to "/etc/dconf/db/local.d/locks/00-security-settings-lock" to prevent user modification:

```
/org/gnome/desktop/media-handling/automount-open
```

Then update the dconf system databases:

```
$ sudo dconf update
```

Additional Information:

CCI-000778 Uniquely identify organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 :: IA-3
- NIST SP 800-53 Revision 4 :: IA-3
- NIST SP 800-53 Revision 5 :: IA-3
- NIST SP 800-53A :: IA-3.1 (ii)

CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4 :: IA-3
- NIST SP 800-53 Revision 5 :: IA-3

1.241 RHEL-09-271030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must disable the graphical user interface autorun function unless required.

```
GROUP ID: V-258016
RULE ID: SV-258016r958804
```

Rationale:

Allowing autorun commands to execute may introduce malicious code to a system. Configuring this setting prevents autorun commands from executing.

Audit:

Verify RHEL 9 disables the graphical user interface autorun function with the following command:
Note: This requirement assumes the use of the RHEL 9 default graphical user interface, the GNOME desktop environment. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

```
$ gsettings get org.gnome.desktop.media-handling autorun-never

true
```

If "autorun-never" is set to "false", and is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Configure the GNOME desktop to disable the autorun function on removable media.
The dconf settings can be edited in the /etc/dconf/db/* location.
Update the [org/gnome/desktop/media-handling] section of the "/etc/dconf/db/local.d/00-security-settings" database file and add or update the following lines:

```
[org/gnome/desktop/media-handling]
autorun-never=true
```

Then update the dconf system databases:

```
$ sudo dconf update
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.242 RHEL-09-271035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent a user from overriding the disabling of the graphical user interface autorun function.

```
GROUP ID: V-258017
RULE ID: SV-258017r1045088
```

Rationale:

Techniques used to address this include protocols using nonces (e.g., numbers generated for a specific one-time use) or challenges (e.g., TLS, WS_Security). Additional techniques include time-synchronous or challenge-response one-time authenticators.

Satisfies: SRG-OS-000114-GPOS-00059, SRG-OS-000378-GPOS-00163, SRG-OS-000480-GPOS-00227

Audit:

Note: This requirement assumes the use of the RHEL 9 default graphical user interface, the GNOME desktop environment. If the system does not have any graphical user interface installed, this requirement is Not Applicable.
Verify RHEL 9 disables ability of the user to override the graphical user interface autorun setting.
Determine which profile the system database is using with the following command:

```
$ gsettings writable org.gnome.desktop.media-handling autorun-never

false
```

If "autorun-never" is writable, the result is "true". If this is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Configure the GNOME desktop to not allow a user to change the setting that disables autorun on removable media.
Add the following line to "/etc/dconf/db/local.d/locks/00-security-settings-lock" to prevent user modification:

```
/org/gnome/desktop/media-handling/autorun-never
```

Then update the dconf system databases:

```
$ sudo dconf update
```

Additional Information:

CCI-000778 Uniquely identify organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 :: IA-3
- NIST SP 800-53 Revision 4 :: IA-3
- NIST SP 800-53 Revision 5 :: IA-3
- NIST SP 800-53A :: IA-3.1 (ii)

CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4 :: IA-3
- NIST SP 800-53 Revision 5 :: IA-3

1.243 RHEL-09-271040 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

RHEL 9 must not allow unattended or automatic logon via the graphical user interface.

```
GROUP ID: V-258018
RULE ID: SV-258018r1045090
```

Rationale:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Audit:

Note: This requirement assumes the use of the RHEL 9 default graphical user interface, the GNOME desktop environment. If the system does not have any graphical user interface installed, this requirement is Not Applicable.
Verify RHEL 9 does not allow an unattended or automatic logon to the system via a graphical user interface.
Check for the value of the "AutomaticLoginEnable" in the "/etc/gdm/custom.conf" file with the following command:

```
$  grep -i automaticlogin /etc/gdm/custom.conf

AutomaticLoginEnable=false
```

If the value of "AutomaticLoginEnable" is not set to "false", this is a finding.

Remediation:

Configure the GNOME desktop display manager to disable automatic login.
Set AutomaticLoginEnable to false in the [daemon] section in /etc/gdm/custom.conf. For example:

```
[daemon]
AutomaticLoginEnable=false
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.244 RHEL-09-271045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must be able to initiate directly a session lock for all connection types using smart card when the smart card is removed.

```
GROUP ID: V-258019
RULE ID: SV-258019r1045092
```

Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined. Rather than be forced to wait for a period of time to expire before the user session can be locked, RHEL 9 needs to provide users with the ability to manually invoke a session lock so users can secure their session if it is necessary to temporarily vacate the immediate physical vicinity.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

Audit:

Note: This requirement assumes the use of the RHEL 9 default graphical user interface, the GNOME desktop environment. If the system does not have any graphical user interface installed, this requirement is Not Applicable.
Verify RHEL 9 enables a user's session lock until that user reestablishes access using established identification and authentication procedures with the following command:

```
$ gsettings get org.gnome.settings-daemon.peripherals.smartcard removal-
action

'lock-screen'
```

If the result is not 'lock-screen', this is a finding.

Remediation:

Configure RHEL 9 to enable a user's session lock until that user re-establishes access using established identification and authentication procedures.
Select or create an authselect profile and incorporate the "with-smartcard-lock-on-removal" feature with the following example:

```
$ sudo authselect select sssd with-smartcard with-smartcard-lock-on-removal
```

Alternatively, the dconf settings can be edited in the /etc/dconf/db/* location.
Add or update the [org/gnome/settings-daemon/peripherals/smartcard] section of the /etc/dconf/db/local.d/00-security-settings" database file and add or update the following lines:

```
[org/gnome/settings-daemon/peripherals/smartcard]
removal-action='lock-screen'
```

Then update the dconf system databases:

```
$ sudo dconf update
```

Additional Information:

CCI-000056 Retain the device lock until the user reestablishes access using established identification and authentication procedures.

- NIST SP 800-53 :: AC-11 b
- NIST SP 800-53 Revision 4 :: AC-11 b
- NIST SP 800-53 Revision 5 :: AC-11 b
- NIST SP 800-53A :: AC-11.1 (iii)

CCI-000057 The information system initiates a session lock after the organization-defined time period of inactivity.

- NIST SP 800-53 :: AC-11 a
- NIST SP 800-53 Revision 4 :: AC-11 a
- NIST SP 800-53 Revision 5 :: AC-11 a
- NIST SP 800-53A :: AC-11.1 (ii)

CCI-000058 The information system provides the capability for users to directly initiate session lock mechanisms.

- NIST SP 800-53 :: AC-11 a
- NIST SP 800-53 Revision 4 :: AC-11 a
- NIST SP 800-53A :: AC-11

1.245 RHEL-09-271050 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent a user from overriding the disabling of the graphical user smart card removal action.

```
GROUP ID: V-258020
RULE ID: SV-258020r1045094
```

Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined. Rather than be forced to wait for a period of time to expire before the user session can be locked, RHEL 9 needs to provide users with the ability to manually invoke a session lock so users can secure their session if it is necessary to temporarily vacate the immediate physical vicinity.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

Audit:

Note: This requirement assumes the use of the RHEL 9 default graphical user interface, the GNOME desktop environment. If the system does not have any graphical user interface installed, this requirement is Not Applicable.
Verify RHEL 9 disables ability of the user to override the smart card removal action setting.

```
$ gsettings writable org.gnome.settings-daemon.peripherals.smartcard removal-
action

false
```

If "removal-action" is writable and the result is "true", this is a finding.

Remediation:

Add the following line to "/etc/dconf/db/local.d/locks/00-security-settings-lock" to prevent user override of the smart card removal action:

```
/org/gnome/settings-daemon/peripherals/smartcard/removal-action
```

Then update the dconf system databases:

```
$ sudo dconf update
```

Additional Information:

CCI-000056 Retain the device lock until the user reestablishes access using established identification and authentication procedures.

- NIST SP 800-53 :: AC-11 b
- NIST SP 800-53 Revision 4 :: AC-11 b
- NIST SP 800-53 Revision 5 :: AC-11 b
- NIST SP 800-53A :: AC-11.1 (iii)

CCI-000057 The information system initiates a session lock after the organization-defined time period of inactivity.

- NIST SP 800-53 :: AC-11 a
- NIST SP 800-53 Revision 4 :: AC-11 a
- NIST SP 800-53 Revision 5 :: AC-11 a
- NIST SP 800-53A :: AC-11.1 (ii)

CCI-000058 The information system provides the capability for users to directly initiate session lock mechanisms.

- NIST SP 800-53 :: AC-11 a
- NIST SP 800-53 Revision 4 :: AC-11 a
- NIST SP 800-53A :: AC-11

1.246 RHEL-09-271055 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must enable a user session lock until that user re-establishes access using established identification and authentication procedures for graphical user sessions.

```
GROUP ID: V-258021
RULE ID: SV-258021r1015088
```

Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

Regardless of where the session lock is determined and implemented, once invoked, the session lock must remain in place until the user reauthenticates. No other activity aside from reauthentication must unlock the system.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

Audit:

Verify RHEL 9 enables a user's session lock until that user re-establishes access using established identification and authentication procedures with the following command: Note: This requirement assumes the use of the RHEL 9 default graphical user interface, the GNOME desktop environment. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

```
$ gsettings get org.gnome.desktop.screensaver lock-enabled

true
```

If the setting is "false", this is a finding.

Remediation:

Configure RHEL 9 to enable a user's session lock until that user re-establishes access using established identification and authentication procedures.
Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following example:

```
$ sudo vi /etc/dconf/db/local.d/00-screensaver
```

Edit the "[org/gnome/desktop/screensaver]" section of the database file and add or update the following lines:

```
# Set this to true to lock the screen when the screensaver activates
lock-enabled=true
```

Update the system databases:

```
$ sudo dconf update
```

Additional Information:

CCI-000056 Retain the device lock until the user reestablishes access using established identification and authentication procedures.

- NIST SP 800-53 :: AC-11 b
- NIST SP 800-53 Revision 4 :: AC-11 b
- NIST SP 800-53 Revision 5 :: AC-11 b
- NIST SP 800-53A :: AC-11.1 (iii)

CCI-000057 The information system initiates a session lock after the organization-defined time period of inactivity.

- NIST SP 800-53 :: AC-11 a
- NIST SP 800-53 Revision 4 :: AC-11 a
- NIST SP 800-53 Revision 5 :: AC-11 a
- NIST SP 800-53A :: AC-11.1 (ii)

CCI-000058 The information system provides the capability for users to directly initiate session lock mechanisms.

- NIST SP 800-53 :: AC-11 a
- NIST SP 800-53 Revision 4 :: AC-11 a
- NIST SP 800-53A :: AC-11

1.247 RHEL-09-271060 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent a user from overriding the screensaver lock-enabled setting for the graphical user interface.

```
GROUP ID: V-258022
RULE ID: SV-258022r1045097
```

Rationale:

A session time-out lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their operating system session prior to vacating the vicinity, operating systems need to be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Implementing session settings will have little value if a user is able to manipulate these settings from the defaults prescribed in the other requirements of this implementation guide.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

Audit:

Note: This requirement assumes the use of the RHEL 9 default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.
Verify RHEL 9 prevents a user from overriding settings for graphical user interfaces.

```
$ gsettings writable org.gnome.desktop.screensaver lock-enabled

false
```

If "lock-enabled" is writable and the result is "true", this is a finding.

Remediation:

Configure RHEL 9 to prevent a user from overriding settings for graphical user interfaces.
Create a database to contain the systemwide screensaver settings (if it does not already exist) with the following command:
Note: The example below is using the database "local" for the system. If the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
$ sudo touch /etc/dconf/db/local.d/locks/session
```

Add the following setting to prevent nonprivileged users from modifying it:

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

Run the following command to update the database:

```
$ sudo dconf update
```

Additional Information:

CCI-000056 Retain the device lock until the user reestablishes access using established identification and authentication procedures.

- NIST SP 800-53 :: AC-11 b
- NIST SP 800-53 Revision 4 :: AC-11 b
- NIST SP 800-53 Revision 5 :: AC-11 b
- NIST SP 800-53A :: AC-11.1 (iii)

CCI-000057 The information system initiates a session lock after the organization-defined time period of inactivity.

- NIST SP 800-53 :: AC-11 a
- NIST SP 800-53 Revision 4 :: AC-11 a
- NIST SP 800-53 Revision 5 :: AC-11 a
- NIST SP 800-53A :: AC-11.1 (ii)

CCI-000058 The information system provides the capability for users to directly initiate session lock mechanisms.

- NIST SP 800-53 :: AC-11 a
- NIST SP 800-53 Revision 4 :: AC-11 a
- NIST SP 800-53A :: AC-11

1.248 RHEL-09-271065 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must automatically lock graphical user sessions after 15 minutes of inactivity.

GROUP ID: V-258023 RULE ID: SV-258023r958402

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 logout 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, the GNOME desktop can be configured to identify when a user's session has idled and take action to initiate a session lock.

Satisfies: SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012

Audit:

Verify RHEL 9 initiates a session lock after a 15-minute period of inactivity for graphical user interfaces with the following command:
Note: This requirement assumes the use of the RHEL 9 default graphical user interface, the GNOME desktop environment. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

```
$ sudo gsettings get org.gnome.desktop.session idle-delay

uint32 900
```

If "idle-delay" is set to "0" or a value greater than "900", this is a finding.

Remediation:

Configure RHEL 9 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:

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

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

```
[org/gnome/desktop/session]
# Set the lock time out to 900 seconds before the session is considered idle
idle-delay=uint32 900
```

Update the system databases:

```
$ sudo dconf update
```

Additional Information:

CCI-000057 The information system initiates a session lock after the organization-defined time period of inactivity.

- NIST SP 800-53 :: AC-11 a
- NIST SP 800-53 Revision 4 :: AC-11 a
- NIST SP 800-53 Revision 5 :: AC-11 a
- NIST SP 800-53A :: AC-11.1 (ii)

CCI-000060 Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

- NIST SP 800-53 :: AC-11 (1)
- NIST SP 800-53 Revision 4 :: AC-11 (1)
- NIST SP 800-53 Revision 5 :: AC-11 (1)
- NIST SP 800-53A :: AC-11 (1).1

1.249 RHEL-09-271070 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent a user from overriding the session idle-delay setting for the graphical user interface.

```
GROUP ID: V-258024
RULE ID: SV-258024r1045100
```

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 logout 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, the GNOME desktop can be configured to identify when a user's session has idled and take action to initiate the session lock. As such, users should not be allowed to change session settings.

Satisfies: SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012

Audit:

Note: This requirement assumes the use of the RHEL 9 default graphical user interface, the GNOME desktop environment. If the system does not have any graphical user interface installed, this requirement is Not Applicable.
Verify RHEL 9 prevents a user from overriding settings for graphical user interfaces.

```
$ gsettings writable org.gnome.desktop.session idle-delay

false
```

If "idle-delay" is writable and the result is "true", this is a finding.

Remediation:

Configure RHEL 9 to prevent a user from overriding settings for graphical user interfaces.
Create a database to contain the systemwide screensaver settings (if it does not already exist) with the following command:
Note: The example below is using the database "local" for the system. If the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
$ sudo touch /etc/dconf/db/local.d/locks/session
```

Add the following setting to prevent nonprivileged users from modifying it:

```
/org/gnome/desktop/session/idle-delay
```

Run the following command to update the database:

```
$ sudo dconf update
```

Additional Information:

CCI-000057 The information system initiates a session lock after the organization-defined time period of inactivity.

- NIST SP 800-53 :: AC-11 a
- NIST SP 800-53 Revision 4 :: AC-11 a
- NIST SP 800-53 Revision 5 :: AC-11 a
- NIST SP 800-53A :: AC-11.1 (ii)

CCI-000060 Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

- NIST SP 800-53 :: AC-11 (1)
- NIST SP 800-53 Revision 4 :: AC-11 (1)
- NIST SP 800-53 Revision 5 :: AC-11 (1)
- NIST SP 800-53A :: AC-11 (1).1

1.250 RHEL-09-271075 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must initiate a session lock for graphical user interfaces when the screensaver is activated.

```
GROUP ID: V-258025
RULE ID: SV-258025r958402
```

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 logout because of the temporary nature of the absence.

Audit:

Verify RHEL 9 initiates a session lock for graphical user interfaces when the screensaver is activated with the following command:
Note: This requirement assumes the use of the RHEL 9 default graphical user interface, the GNOME desktop environment. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

```
$ gsettings get org.gnome.desktop.screensaver lock-delay

uint32 5
```

If the "uint32" setting is not set to "5" or less, or is missing, this is a finding.

Remediation:

Configure RHEL 9 to initiate a session lock for graphical user interfaces when a screensaver is activated.
Create a database to contain the system-wide screensaver settings (if it does not already exist) with the following command:
Note: The example below is using the database "local" for the system, so if the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

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

[org/gnome/desktop/screensaver]
lock-delay=uint32 5
```

The "uint32" must be included along with the integer key values as shown.
Update the system databases:

```
$ sudo dconf update
```

Additional Information:

CCI-000057 The information system initiates a session lock after the organization-defined time period of inactivity.

- NIST SP 800-53 :: AC-11 a
- NIST SP 800-53 Revision 4 :: AC-11 a
- NIST SP 800-53 Revision 5 :: AC-11 a
- NIST SP 800-53A :: AC-11.1 (ii)

1.251 RHEL-09-271080 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent a user from overriding the session lock-delay setting for the graphical user interface.

```
GROUP ID: V-258026
RULE ID: SV-258026r1045103
```

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 logout 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, the GNOME desktop can be configured to identify when a user's session has idled and take action to initiate the session lock. As such, users should not be allowed to change session settings.

Audit:

Note: This requirement assumes the use of the RHEL 9 default graphical user interface, the GNOME desktop environment. If the system does not have any graphical user interface installed, this requirement is Not Applicable.
Verify RHEL 9 prevents a user from overriding settings for graphical user interfaces.

```
$ gsettings writable org.gnome.desktop.screensaver lock-delay

false
```

If "lock-delay" is writable and the result is "true", this is a finding.

Remediation:

Configure RHEL 9 to prevent a user from overriding settings for graphical user interfaces.
Create a database to contain the systemwide screensaver settings (if it does not already exist) with the following command:
Note: The example below is using the database "local" for the system. If the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
$ sudo touch /etc/dconf/db/local.d/locks/session
```

Add the following setting to prevent nonprivileged users from modifying it:

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

Run the following command to update the database:

```
$ sudo dconf update
```

Additional Information:

CCI-000057 The information system initiates a session lock after the organization-defined time period of inactivity.

- NIST SP 800-53 :: AC-11 a
- NIST SP 800-53 Revision 4 :: AC-11 a
- NIST SP 800-53 Revision 5 :: AC-11 a
- NIST SP 800-53A :: AC-11.1 (ii)

1.252 RHEL-09-271085 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must conceal, via the session lock, information previously visible on the display with a publicly viewable image.

```
GROUP ID: V-258027
RULE ID: SV-258027r1045106
```

Rationale:

Setting the screensaver mode to blank-only conceals the contents of the display from passersby.

Audit:

Note: This requirement assumes the use of the RHEL 9 default graphical user interface, the GNOME desktop environment. If the system does not have any graphical user interface installed, this requirement is Not Applicable.
To ensure the screensaver is configured to be blank, run the following command:

```
$ gsettings writable org.gnome.desktop.screensaver picture-uri

false
```

If "picture-uri" is writable and the result is "true", this is a finding.

Remediation:

Configure RHEL 9 to prevent a user from overriding the picture-uri setting for graphical user interfaces.
In the file "/etc/dconf/db/local.d/00-security-settings", add or update the following lines:

```
[org/gnome/desktop/screensaver]
picture-uri=''
```

Prevent user modification by adding the following line to "/etc/dconf/db/local.d/locks/00-security-settings-lock":

```
/org/gnome/desktop/screensaver/picture-uri
```

Update the dconf system databases:

```
$ sudo dconf update
```

Additional Information:

CCI-000060 Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

- NIST SP 800-53 :: AC-11 (1)
- NIST SP 800-53 Revision 4 :: AC-11 (1)
- NIST SP 800-53 Revision 5 :: AC-11 (1)
- NIST SP 800-53A :: AC-11 (1).1

1.253 RHEL-09-271090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 effective dconf policy must match the policy keyfiles.

```
GROUP ID: V-258028
RULE ID: SV-258028r991589
```

Rationale:

Unlike text-based keyfiles, the binary database is impossible to check through most automated and all manual means; therefore, in order to evaluate dconf configuration, both have to be true at the same time - configuration files have to be compliant, and the database needs to be more recent than those keyfiles, which gives confidence that it reflects them.

Audit:

Check the last modification time of the local databases, comparing it to the last modification time of the related keyfiles. The following command will check every dconf database and compare its modification time to the related system keyfiles:
Note: This requirement assumes the use of the RHEL 9 default graphical user interface, the GNOME desktop environment. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

```
$ function dconf_needs_update { for db in $(find /etc/dconf/db -maxdepth 1 -
type f); do db_mtime=$(stat -c %Y "$db"); keyfile_mtime=$(stat -c %Y
"$db".d/* | sort -n | tail -1); if [ -n "$db_mtime" ] && [ -n
"$keyfile_mtime" ] && [ "$db_mtime" -lt "$keyfile_mtime" ]; then echo "$db
needs update"; return 1; fi; done; }; dconf_needs_update
```

If the command has any output, then a dconf database needs to be updated, and this is a finding.

Remediation:

Update the dconf databases by running the following command:

```
$ sudo dconf update
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.254 RHEL-09-271095 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must disable the ability of a user to restart the system from the login screen.

```
GROUP ID: V-258029
RULE ID: SV-258029r1045109
```

Rationale:

A user who is at the console can reboot the system at the login screen. If restart or shutdown buttons are pressed at the login screen, this can create the risk of short-term loss of availability of systems due to reboot.

Audit:

Note: This requirement assumes the use of the RHEL 9 default graphical user interface, Gnome Shell. If the system does not have any graphical user interface installed, this requirement is Not Applicable.
Verify RHEL 9 disables a user's ability to restart the system with the following command:

```
$ gsettings get org.gnome.login-screen disable-restart-buttons

true
```

If "disable-restart-buttons" is "false", this is a finding.

Remediation:

Configure RHEL 9 to disable a user's ability to restart the system.

```
$ gsettings set org.gnome.login-screen disable-restart-buttons true
```

Update the dconf system databases:

```
$ sudo dconf update
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.255 RHEL-09-271100 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent a user from overriding the disable-restart-buttons setting for the graphical user interface.

```
GROUP ID: V-258030
RULE ID: SV-258030r1045112
```

Rationale:

A user who is at the console can reboot the system at the login screen. If restart or shutdown buttons are pressed at the login screen, this can create the risk of short-term loss of availability of systems due to reboot.

Audit:

Note: This requirement assumes the use of the RHEL 9 default graphical user interface, the GNOME desktop environment. If the system does not have any graphical user interface installed, this requirement is Not Applicable.
Verify RHEL 9 prevents a user from overriding the disable-restart-buttons setting for graphical user interfaces.

```
$ gsettings writable org.gnome.login-screen disable-restart-buttons

false
```

If "disable-restart-buttons" is writable and the result is "true", this is a finding.

Remediation:

Configure RHEL 9 to prevent a user from overriding the disable-restart-buttons setting for graphical user interfaces.
Create a database to contain the systemwide graphical user logon settings (if it does not already exist) with the following command:

```
$ sudo touch /etc/dconf/db/local.d/locks/session
```

Add the following line to prevent nonprivileged users from modifying it:

```
/org/gnome/login-screen/disable-restart-buttons
```

Run the following command to update the database:

```
$ sudo dconf update
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.256 RHEL-09-271105 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must disable the ability of a user to accidentally press Ctrl-Alt-Del and cause a system to shut down or reboot.

```
GROUP ID: V-258031
RULE ID: SV-258031r1045114
```

Rationale:

A locally logged-in user who presses Ctrl-Alt-Del, when at the console, can reboot the system. If accidentally pressed, as could happen in the case of mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot.

Audit:

Verify RHEL 9 is configured to ignore the Ctrl-Alt-Del sequence in the GNOME desktop with the following command:
Note: This requirement assumes the use of the RHEL 9 default graphical user interface, the GNOME desktop environment. If the system does not have any graphical user interface installed, this requirement is Not Applicable.

```
$ gsettings get org.gnome.settings-daemon.plugins.media-keys logout

"['']"
```

If the GNOME desktop is configured to shut down when Ctrl-Alt-Del is pressed, this is a finding.

Remediation:

Configure RHEL 9 to ignore the Ctrl-Alt-Del sequence in the GNOME desktop.
Run the following command to set the media-keys logout setting:

```
$ gsettings set org.gnome.settings-daemon.plugins.media-keys logout "['']"
```

Run the following command to update the database:

```
$ sudo dconf update
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.257 RHEL-09-271110 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent a user from overriding the Ctrl-Alt-Del sequence settings for the graphical user interface.

```
GROUP ID: V-258032
RULE ID: SV-258032r1045117
```

Rationale:

A locally logged-in user who presses Ctrl-Alt-Del, when at the console, can reboot the system. If accidentally pressed, as could happen in the case of mixed OS environment, this can create the risk of short-term loss of availability of systems due to unintentional reboot.

Audit:

Note: This requirement assumes the use of the RHEL 9 default graphical user interface, the GNOME desktop environment. If the system does not have any graphical user interface installed, this requirement is Not Applicable.
Verify that users cannot enable the Ctrl-Alt-Del sequence in the GNOME desktop with the following command:

```
$ gsettings writable org.gnome.settings-daemon.plugins.media-keys logout

false
```

If "logout" is writable and the result is "true", this is a finding.

Remediation:

Configure RHEL 9 to disallow the user changing the Ctrl-Alt-Del sequence in the GNOME desktop.
Create a database to contain the systemwide graphical user logon settings (if it does not already exist) with the following command:

```
$ sudo touch /etc/dconf/db/local.d/locks/session
```

Add the following line to the session locks file to prevent nonprivileged users from modifying the Ctrl-Alt-Del setting:

```
/org/gnome/settings-daemon/plugins/media-keys/logout
```

Run the following command to update the database:

```
$ sudo dconf update
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.258 RHEL-09-271115 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must disable the user list at logon for graphical user interfaces.

```
GROUP ID: V-258033
RULE ID: SV-258033r1045120
```

Rationale:

Leaving the user list enabled is a security risk since it allows anyone with physical access to the system to enumerate known user accounts without authenticated access to the system.

Audit:

Note: This requirement assumes the use of the RHEL 9 default graphical user interface, the GNOME desktop environment. If the system does not have any graphical user interface installed, this requirement is Not Applicable.
Verify that RHEL 9 disables the user logon list for graphical user interfaces with the following command:

```
$ gsettings get org.gnome.login-screen disable-user-list

true
```

If the setting is "false", this is a finding.

Remediation:

Configure RHEL 9 to disable the user list at logon for graphical user interfaces.
Create a database to contain the systemwide screensaver settings (if it does not already exist) with the following command:
Note: The example below is using the database "local" for the system. If the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
$ sudo touch /etc/dconf/db/local.d/02-login-screen

[org/gnome/login-screen]
disable-user-list=true
```

Update the system databases:

```
$ sudo dconf update
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.259 RHEL-09-291010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must be configured to disable USB mass storage.

```
GROUP ID: V-258034
RULE ID: SV-258034r1051267
```

Rationale:

USB mass storage 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:

Verify that RHEL 9 disables the ability to load the USB Storage kernel module with the following command:

```
$ grep -r usb-storage /etc/modprobe.conf /etc/modprobe.d/*

install usb-storage /bin/false
blacklist usb-storage
```

If the command does not return any output, or either line is commented out, and use of USB Storage is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Remediation:

To configure the system to prevent the usb-storage kernel module from being loaded, add the following lines to the file "/etc/modprobe.d/usb-storage.conf" (or create "usb-storage.conf" if it does not exist):

```
install usb-storage /bin/false
blacklist usb-storage
```

Additional Information:

CCI-000778 Uniquely identify organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 :: IA-3
- NIST SP 800-53 Revision 4 :: IA-3
- NIST SP 800-53 Revision 5 :: IA-3
- NIST SP 800-53A :: IA-3.1 (ii)

CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4 :: IA-3
- NIST SP 800-53 Revision 5 :: IA-3

CCI-003959 Prohibit the use or connection of unauthorized hardware components.

- NIST SP 800-53 Revision 5 :: CM-7 (9) (b)

1.260 RHEL-09-291015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must have the USBGuard package installed.

```
GROUP ID: V-258035
RULE ID: SV-258035r1045125
```

Rationale:

The USBguard-daemon is the main component of the USBGuard software framework. It runs as a service in the background and enforces the USB device authorization policy for all USB devices. The policy is defined by a set of rules using a rule language described in the usbguard-rules.conf file. The policy and the authorization state of USB devices can be modified during runtime using the usbguard tool.

The system administrator (SA) must work with the site information system security officer (ISSO) to determine a list of authorized peripherals and establish rules within the USBGuard software framework to allow only authorized devices.

Audit:

Verify USBGuard is installed on the operating system with the following command:

```
$ sudo dnf list installed usbguard
```

Example output:

```
Installed Packages
usbguard.x86_64          1.0.0-10.el9_1.2          @rhel-9-for-x86_64-
appstream-rpms
```

If the USBGuard package is not installed, ask the SA to indicate how unauthorized peripherals are being blocked.
If there is no evidence that unauthorized peripherals are being blocked before establishing a connection, this is a finding.
If the system is virtual machine with no virtual or physical USB peripherals attached, this is not a finding.

Remediation:

Install the usbguard package with the following command:

```
$ sudo dnf install usbguard
```

Enable the service to start on boot and then start it with the following commands:

```
$ sudo systemctl enable usbguard
$ sudo systemctl start usbguard
```

Verify the status of the service with the following command:

```
$ sudo systemctl status usbguard
```

Note: usbguard will need to be configured to allow authorized devices once it is enabled on RHEL 9.

Additional Information:

CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4 :: IA-3
- NIST SP 800-53 Revision 5 :: IA-3

CCI-003959 Prohibit the use or connection of unauthorized hardware components.

- NIST SP 800-53 Revision 5 :: CM-7 (9) (b)

1.261 RHEL-09-291020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must have the USBGuard package enabled.

```
GROUP ID: V-258036
RULE ID: SV-258036r1014861
```

Rationale:

The USBguard-daemon is the main component of the USBGuard software framework. It runs as a service in the background and enforces the USB device authorization policy for all USB devices. The policy is defined by a set of rules using a rule language described in the usbguard-rules.conf file. The policy and the authorization state of USB devices can be modified during runtime using the usbguard tool.

The system administrator (SA) must work with the site information system security officer (ISSO) to determine a list of authorized peripherals and establish rules within the USBGuard software framework to allow only authorized devices.

Audit:

Verify RHEL 9 has USBGuard enabled with the following command:

```
$ systemctl is-active usbguard

active
```

If usbguard is not active, ask the SA to indicate how unauthorized peripherals are being blocked.
If there is no evidence that unauthorized peripherals are being blocked before establishing a connection, this is a finding.
If the system is virtual machine with no virtual or physical USB peripherals attached, this is not a finding.

Remediation:

To enable the USBGuard service run the following command:

```
$ sudo systemctl enable --now usbguard
```

Additional Information:

CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4 :: IA-3
- NIST SP 800-53 Revision 5 :: IA-3

CCI-003959 Prohibit the use or connection of unauthorized hardware components.

- NIST SP 800-53 Revision 5 :: CM-7 (9) (b)

1.262 RHEL-09-291025 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

RHEL 9 must enable Linux audit logging for the USBGuard daemon.

```
GROUP ID: V-258037
RULE ID: SV-258037r1014863
```

Rationale:

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

If auditing is enabled late in the startup process, the actions of some startup processes may not be audited. Some audit systems also maintain state information only available if auditing is enabled before a given process is created.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records.

DOD has defined the list of events for which RHEL 9 will provide an audit record generation capability as the following:

1. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels);
2. Access actions, such as successful and unsuccessful logon attempts, privileged activities or other system-level access, starting and ending time for user access to the system, concurrent logons from different workstations, successful and unsuccessful accesses to objects, all program initiations, and all direct access to the information system;
3. All account creations, modifications, disabling, and terminations; and
4. All kernel module load, unload, and restart actions.

Audit:

To verify that Linux Audit logging is enabled for the USBGuard daemon with the following command:

```
$ sudo grep AuditBackend /etc/usbguard/usbguard-daemon.conf

AuditBackend=LinuxAudit
```

If "AuditBackend" is not set to "LinuxAudit", this is a finding.
If the system is virtual machine with no virtual or physical USB peripherals attached, this is not a finding.

Remediation:

Configure RHEL 9 USBGuard AuditBackend to use the audit system.
Add or edit the following line in /etc/usbguard/usbguard-daemon.conf

```
AuditBackend=LinuxAudit
```

Additional Information:

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

1.263 RHEL-09-291030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must block unauthorized peripherals before establishing a connection.

```
GROUP ID: V-258038
RULE ID: SV-258038r1045128
```

Rationale:

The USBguard-daemon is the main component of the USBGuard software framework. It runs as a service in the background and enforces the USB device authorization policy for all USB devices. The policy is defined by a set of rules using a rule language described in the usbguard-rules.conf file. The policy and the authorization state of USB devices can be modified during runtime using the usbguard tool.

The system administrator (SA) must work with the site information system security officer (ISSO) to determine a list of authorized peripherals and establish rules within the USBGuard software framework to allow only authorized devices.

Audit:

Note: If the system is virtual machine with no virtual or physical USB peripherals attached, this is Not Applicable.
Verify the USBGuard has a policy configured with the following command:

```
$ sudo usbguard list-rules

allow id 1d6b:0001 serial
```

If the command does not return results or an error is returned, ask the SA to indicate how unauthorized peripherals are being blocked.
If there is no evidence that unauthorized peripherals are being blocked before establishing a connection, this is a finding.

Remediation:

Configure the operating system to enable the blocking of unauthorized peripherals with the following command:
Note: This command must be run from a root shell and will create an allow list for any usb devices currently connected to the system.

```
# usbguard generate-policy --no-hash > /etc/usbguard/rules.conf
```

Note: Enabling and starting usbguard without properly configuring it for an individual system will immediately prevent any access over a usb device such as a keyboard or mouse.

Additional Information:

CCI-001958 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

- NIST SP 800-53 Revision 4 :: IA-3
- NIST SP 800-53 Revision 5 :: IA-3

1.264 RHEL-09-291035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 Bluetooth must be disabled.

```
GROUP ID: V-258039
RULE ID: SV-258039r1045131
```

Rationale:

This requirement applies to wireless peripheral technologies (e.g., wireless mice, keyboards, displays, etc.) used with RHEL 9 systems. Wireless peripherals (e.g., Wi-Fi/Bluetooth/IR keyboards, mice and pointing devices, and near field communications [NFC]) present a unique challenge by creating an open, unsecured port on a computer. Wireless peripherals must meet DOD requirements for wireless data transmission and be approved for use by the Authorizing Official (AO). Even though some wireless peripherals, such as mice and pointing devices, do not ordinarily carry information that need to be protected, modification of communications with these wireless peripherals may be used to compromise the RHEL 9 operating system.

Satisfies: SRG-OS-000095-GPOS-00049, SRG-OS-000300-GPOS-00118

Audit:

Verify that RHEL 9 disables the ability to load the Bluetooth kernel module with the following command:

```
$ sudo grep -r bluetooth /etc/modprobe.conf /etc/modprobe.d/*

install bluetooth /bin/false
blacklist Bluetooth
```

If the command does not return any output, or the lines are commented out, and use of Bluetooth is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Configure RHEL 9 to disable the Bluetooth adapter when not in use.
Create or modify the "/etc/modprobe.d/bluetooth.conf" file with the following lines:

```
install bluetooth /bin/false
blacklist bluetooth
```

Reboot the system for the settings to take effect.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53 :: CM-7
- NIST SP 800-53 Revision 4 :: CM-7 a
- NIST SP 800-53 Revision 5 :: CM-7 a
- NIST SP 800-53A :: CM-7.1 (ii)

CCI-001443 Protect wireless access to the system using authentication of users and/or devices.

- NIST SP 800-53 :: AC-18 (1)
- NIST SP 800-53 Revision 4 :: AC-18 (1)
- NIST SP 800-53 Revision 5 :: AC-18 (1)
- NIST SP 800-53A :: AC-18 (1).1

1.265 RHEL-09-291040 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 wireless network adapters must be disabled.

```
GROUP ID: V-258040
RULE ID: SV-258040r991568
```

Rationale:

This requirement applies to wireless peripheral technologies (e.g., wireless mice, keyboards, displays, etc.) used with RHEL 9 systems. Wireless peripherals (e.g., Wi-Fi/Bluetooth/IR keyboards, mice and pointing devices, and near field communications [NFC]) present a unique challenge by creating an open, unsecured port on a computer. Wireless peripherals must meet DOD requirements for wireless data transmission and be approved for use by the Authorizing Official (AO). Even though some wireless peripherals, such as mice and pointing devices, do not ordinarily carry information that need to be protected, modification of communications with these wireless peripherals may be used to compromise the RHEL 9 operating system.

Satisfies: SRG-OS-000299-GPOS-00117, SRG-OS-000300-GPOS-00118, SRG-OS-000424-GPOS-00188, SRG-OS-000481-GPOS-00481

Audit:

Verify there are no wireless interfaces configured on the system with the following command:
Note: This requirement is Not Applicable for systems that do not have physical wireless network radios.

```
$ nmcli device status

DEVICE                     TYPE            STATE                    CONNECTION
virbr0                       bridge         connected              virbr0
wlp7s0                     wifi              connected             wifiSSID
enp6s0                     ethernet     disconnected        --
p2p-dev-wlp7s0     wifi-p2p     disconnected        --
lo                              loopback    unmanaged           --
virbr0-nic                 tun               unmanaged          --
```

If a wireless interface is configured and has not been documented and approved by the information system security officer (ISSO), this is a finding.

Remediation:

Configure the system to disable all wireless network interfaces with the following command:

```
$ nmcli radio all off
```

Additional Information:

CCI-001443 Protect wireless access to the system using authentication of users and/or devices.

- NIST SP 800-53 :: AC-18 (1)
- NIST SP 800-53 Revision 4 :: AC-18 (1)
- NIST SP 800-53 Revision 5 :: AC-18 (1)
- NIST SP 800-53A :: AC-18 (1).1

CCI-001444 Protect wireless access to the system using encryption.

- NIST SP 800-53 :: AC-18 (1)
- NIST SP 800-53 Revision 4 :: AC-18 (1)
- NIST SP 800-53 Revision 5 :: AC-18 (1)
- NIST SP 800-53A :: AC-18 (1).1

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4 :: SC-8
- NIST SP 800-53 Revision 5 :: SC-8

CCI-002421 Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4 :: SC-8 (1)
- NIST SP 800-53 Revision 5 :: SC-8 (1)

1.266 RHEL-09-411010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 user account passwords for new users or password changes must have a 60-day maximum password lifetime restriction in /etc/login.defs.

```
GROUP ID: V-258041
RULE ID: SV-258041r1038967
```

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.

Setting the password maximum age ensures users are required to periodically change their passwords. Requiring shorter password lifetimes increases the risk of users writing down the password in a convenient location subject to physical compromise.

Audit:

Verify that RHEL 9 enforces a 60-day maximum password lifetime for new user accounts by running the following command:

```
$ grep -i pass_max_days /etc/login.defs

PASS_MAX_DAYS 60
```

If the "PASS_MAX_DAYS" parameter value is greater than "60", or commented out, this is a finding.

Remediation:

Configure RHEL 9 to enforce a 60-day maximum password lifetime.
Add or modify the following line in the "/etc/login.defs" file:

```
PASS_MAX_DAYS 60
```

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000199 The information system enforces maximum password lifetime restrictions.

- NIST SP 800-53 :: IA-5 (1) (d)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (d)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.267 RHEL-09-411015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 user account passwords must have a 60-day maximum password lifetime restriction.

```
GROUP ID: V-258042
RULE ID: SV-258042r1045133
```

Rationale:

Any password, no matter how complex, can eventually be cracked; therefore, passwords need to be changed periodically. If RHEL 9 does not limit the lifetime of passwords and force users to change their passwords, there is the risk that RHEL 9 passwords could be compromised.

Audit:

Verify the maximum time period for existing passwords is restricted to 60 days with the following commands:

```
$ sudo awk -F: '$5 > 60 {printf "%s %d\n", $1, $5}' /etc/shadow

$ sudo awk -F: '$5 <= 0 {printf "%s %d\n", $1, $5}' /etc/shadow
```

If any results are returned that are not associated with a system account, this is a finding.

Remediation:

Configure noncompliant accounts to enforce a 60-day maximum password lifetime restriction.

```
passwd -x 60 [user]
```

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000199 The information system enforces maximum password lifetime restrictions.

- NIST SP 800-53 :: IA-5 (1) (d)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (d)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.268 RHEL-09-411020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

All RHEL 9 local interactive user accounts must be assigned a home directory upon creation.

```
GROUP ID: V-258043
RULE ID: SV-258043r991589
```

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 RHEL 9 are assigned a home directory upon creation with the following command:

```
$ grep -i create_home /etc/login.defs

CREATE_HOME yes
```

If the value for "CREATE_HOME" parameter is not set to "yes", the line is missing, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to assign home directories to all new local interactive users by setting the "CREATE_HOME" parameter in "/etc/login.defs" to "yes" as follows.

```
CREATE_HOME yes
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.269 RHEL-09-411025 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must set the umask value to 077 for all local interactive user accounts.

```
GROUP ID: V-258044
RULE ID: SV-258044r1045135
```

Rationale:

The umask controls the default access mode assigned to newly created files. A umask of 077 limits new files to mode 600 or less permissive. Although umask can be represented as a four-digit number, the first digit representing special access modes is typically ignored or required to be "0". This requirement applies to the globally configured system defaults and the local interactive user defaults for each account on the system.

Audit:

Verify that the default umask for all local interactive users is "077".
Identify the locations of all local interactive user home directories by looking at the "/etc/passwd" file.
Check all local interactive user initialization files for interactive users with the following command:
Note: The example is for a system that is configured to create users home directories in the "/home" directory.

```
$ sudo find /home -maxdepth 2 -type f -name ".[^.]*" -exec grep -iH -d skip -
-exclude=.bash_history umask {} \;

/home/wadea/.bash_history:grep -i umask /etc/bashrc /etc/csh.cshrc
/etc/profile
/home/wadea/.bash_history:grep -i umask /etc/login.defs
```

If any local interactive user initialization files are found to have a umask statement that sets a value less restrictive than "077", this is a finding.

Remediation:

Remove the umask statement from all local interactive user's initialization files.
If the account is for an application, the requirement for a umask less restrictive than "077" can be documented with the information system security officer, but the user agreement for access to the account must specify that the local interactive user must log on to their account first and then switch the user to the application account with the correct option to gain the account's environment variables.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.270 RHEL-09-411030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 duplicate User IDs (UIDs) must not exist for interactive users.

```
GROUP ID: V-258045
RULE ID: SV-258045r958482
```

Rationale:

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

Satisfies: SRG-OS-000104-GPOS-00051, SRG-OS-000121-GPOS-00062, SRG-OS-000042-GPOS-00020

Audit:

Verify that RHEL 9 contains no duplicate UIDs for interactive users with the following command:

```
$ sudo awk -F ":" 'list[$3]++{print $1, $3}' /etc/passwd
```

If output is produced and the accounts listed are interactive user accounts, this is a finding.

Remediation:

Edit the file "/etc/passwd" and provide each interactive user account that has a duplicate UID with a unique UID.

Additional Information:

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53 :: IA-2
- NIST SP 800-53 Revision 4 :: IA-2
- NIST SP 800-53 Revision 5 :: IA-2
- NIST SP 800-53A :: IA-2.1

CCI-000804 Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

- NIST SP 800-53 :: IA-8
- NIST SP 800-53 Revision 4 :: IA-8
- NIST SP 800-53 Revision 5 :: IA-8
- NIST SP 800-53A :: IA-8.1

1.271 RHEL-09-411035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 system accounts must not have an interactive login shell.

```
GROUP ID: V-258046
RULE ID: SV-258046r991589
```

Rationale:

Ensuring shells are not given to system accounts upon login makes it more difficult for attackers to make use of system accounts.

Audit:

Verify that system accounts must not have an interactive login shell with the following command:

```
$ awk -F: '($3<1000){print $1 ":" $3 ":" $7}' /etc/passwd

root:0:/bin/bash
bin:1:/sbin/nologin
daemon:2:/sbin/nologin
adm:3:/sbin/nologin
lp:4:/sbin/nologin
```

Identify the system accounts from this listing that do not have a nologin shell.
If any system account (other than the root account) has a login shell and it is not documented with the information system security officer (ISSO), this is a finding.

Remediation:

Configure RHEL 9 so that all noninteractive accounts on the system do not have an interactive shell assigned to them.
If the system account needs a shell assigned for mission operations, document the need with the information system security officer (ISSO).
Run the following command to disable the interactive shell for a specific noninteractive user account:
Replace with the user that has a login shell.

```
$ sudo usermod --shell /sbin/nologin <user>
```

Do not perform the steps in this section on the root account. Doing so will cause the system to become inaccessible.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.272 RHEL-09-411040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must automatically expire temporary accounts within 72 hours.

```
GROUP ID: V-258047
RULE ID: SV-258047r958508
```

Rationale:

Temporary accounts are privileged or nonprivileged accounts that are established during pressing circumstances, such as new software or hardware configuration or an incident response, where the need for prompt account activation requires bypassing normal account authorization procedures. If any inactive temporary accounts are left enabled on the system and are not either manually removed or automatically expired within 72 hours, the security posture of the system will be degraded and exposed to exploitation by unauthorized users or insider threat actors.

Temporary accounts are different from emergency accounts. Emergency accounts, also known as "last resort" or "break glass" accounts, are local logon accounts enabled on the system for emergency use by authorized system administrators to manage a system when standard logon methods are failing or not available. Emergency accounts are not subject to manual removal or scheduled expiration requirements.

The automatic expiration of temporary accounts may be extended as needed by the circumstances but it must not be extended indefinitely. A documented permanent account should be established for privileged users who need long-term maintenance accounts.

Satisfies: SRG-OS-000123-GPOS-00064, SRG-OS-000002-GPOS-00002

Audit:

Verify temporary accounts have been provisioned with an expiration date of 72 hours. For every existing temporary account, run the following command to obtain its account expiration information:

```
$ sudo chage -l <temporary_account_name> | grep -i "account expires"
```

Verify each of these accounts has an expiration date set within 72 hours.
If any temporary accounts have no expiration date set or do not expire within 72 hours, this is a finding.

Remediation:

Configure the operating system to expire temporary accounts after 72 hours with the following command:

```
$ sudo chage -E $(date -d +3days +%Y-%m-%d) <temporary_account_name>
```

Additional Information:

CCI-000016 Automatically remove or disable temporary and emergency accounts after an organization-defined time-period for each type of account.

- NIST SP 800-53 :: AC-2 (2)
- NIST SP 800-53 Revision 4 :: AC-2 (2)
- NIST SP 800-53 Revision 5 :: AC-2 (2)
- NIST SP 800-53A :: AC-2 (2).1 (ii)

CCI-001682 Automatically removes or disables emergency accounts after an organization-defined time period for each type of account.

- NIST SP 800-53 :: AC-2 (2)
- NIST SP 800-53 Revision 4 :: AC-2 (2)
- NIST SP 800-53 Revision 5 :: AC-2 (2)
- NIST SP 800-53A :: AC-2 (2).1 (ii)

1.273 RHEL-09-411045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

All RHEL 9 interactive users must have a primary group that exists.

```
GROUP ID: V-258048
RULE ID: SV-258048r1069380
```

Rationale:

If a user is assigned the Group Identifier (GID) of a group that does not exist on the system, and a group with the GID is subsequently created, the user may have unintended rights to any files associated with the group.

Audit:

Verify that all RHEL 9 interactive users have a valid GID.
Check that the interactive users have a valid GID with the following command:

```
$ sudo pwck -r
```

If pwck reports "no group" for any interactive user, this is a finding.

Remediation:

Configure the system so that all GIDs are referenced in "/etc/passwd" are defined in "/etc/group".
Edit the file "/etc/passwd" and ensure that every user's GID is a valid GID.

Additional Information:

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53 :: IA-2
- NIST SP 800-53 Revision 4 :: IA-2
- NIST SP 800-53 Revision 5 :: IA-2
- NIST SP 800-53A :: IA-2.1

1.274 RHEL-09-411050 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must disable account identifiers (individuals, groups, roles, and devices) after 35 days of inactivity.

```
GROUP ID: V-258049
RULE ID: SV-258049r1015092
```

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.

Disabling inactive accounts ensures that accounts which may not have been responsibly removed are not available to attackers who may have compromised their credentials.

Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

Audit:

Verify that RHEL 9 account identifiers (individuals, groups, roles, and devices) are disabled after 35 days of inactivity with the following command:
Check the account inactivity value by performing the following command:

```
$ sudo grep -i inactive /etc/default/useradd

INACTIVE=35
```

If "INACTIVE" is set to "-1", a value greater than "35", or is commented out, this is a finding.

Remediation:

Configure RHEL 9 to disable account identifiers after 35 days of inactivity after the password expiration.
Run the following command to change the configuration for useradd:

```
$ sudo useradd -D -f 35
```

The recommendation is 35 days, but a lower value is acceptable.

Additional Information:

CCI-003627 Disable accounts when the accounts have expired.

- NIST SP 800-53 Revision 5 :: AC-2 (3) (a)

CCI-003628 Disable accounts when the accounts are no longer associated to a user.

- NIST SP 800-53 Revision 5 :: AC-2 (3) (b)

CCI-000795 The organization manages information system identifiers by disabling the identifier after an organization-defined time period of inactivity.

- NIST SP 800-53 :: IA-4 e
- NIST SP 800-53 Revision 4 :: IA-4 e
- NIST SP 800-53A :: IA-4.1 (iii)

1.275 RHEL-09-411055 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Executable search paths within the initialization files of all local interactive RHEL 9 users must only contain paths that resolve to the system default or the users home directory.

```
GROUP ID: V-258050
RULE ID: SV-258050r1045137
```

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 users home directory), executables in these directories may be executed instead of system commands.

This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is interpreted as the current working directory. If deviations from the default system search path for the local interactive user are required, they must be documented with the information system security officer (ISSO).

Audit:

Verify that all local interactive user initialization file executable search path statements do not contain statements that will reference a working directory other than user home directories with the following commands:

```
$ sudo find /home -maxdepth 2 -type f -name ".[^.]*" -exec grep -iH path= {}
\;

PATH="$HOME/.local/bin:$HOME/bin:$PATH"
```

If any local interactive user initialization files have executable search path statements that include directories outside of their home directory, and this is not documented with the ISSO as an operational requirement, this is a finding.

Remediation:

Edit the local interactive user initialization files to change any PATH variable statements that reference directories other than their home directory.
If a local interactive user requires path variables to reference a directory owned by the application, it must be documented with the ISSO.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.276 RHEL-09-411060 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

All RHEL 9 local interactive users must have a home directory assigned in the /etc/passwd file.

```
GROUP ID: V-258051
RULE ID: SV-258051r991589
```

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 that interactive users on the system have a home directory assigned with the following command:

```
$ sudo awk -F: '($3>=1000)&&($7 !~ /nologin/){print $1, $3, $6}' /etc/passwd

smithk:x:1000:1000:smithk:/home/smithk:/bin/bash
scsaustin:x:1001:1001:scsaustin:/home/scsaustin:/bin/bash
djohnson:x:1002:1002:djohnson:/home/djohnson:/bin/bash
```

Inspect the output and verify that all interactive users (normally users with a user identifier (UID) greater that 1000) have a home directory defined.
If users home directory is not defined, this is a finding.

Remediation:

Create and assign home directories to all local interactive users on RHEL 9 that currently do not have a home directory assigned.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.277 RHEL-09-411065 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

All RHEL 9 local interactive user home directories defined in the /etc/passwd file must exist.

```
GROUP ID: V-258052
RULE ID: SV-258052r991589
```

Rationale:

If a local interactive user has a home directory defined that does not exist, the user may be given access to the / directory as the current working directory upon logon. This could create a denial of service because the user would not be able to access their logon configuration files, and it may give them visibility to system files they normally would not be able to access.

Audit:

Verify the assigned home directories of all interactive users on the system exist with the following command:

```
$ sudo pwck -r

user 'mailnull': directory 'var/spool/mqueue' does not exist
```

The output should not return any interactive users.
If users home directory does not exist, this is a finding.

Remediation:

Create home directories to all local interactive users that currently do not have a home directory assigned. Use the following commands to create the user home directory assigned in "/etc/ passwd":
Note: The example will be for the user wadea, who has a home directory of "/home/wadea", a user identifier (UID) of "wadea", and a Group Identifier (GID) of "users assigned" in "/etc/passwd".

```
$ sudo mkdir /home/wadea
$ sudo chown wadea /home/wadea
$ sudo chgrp users /home/wadea
$ sudo chmod 0750 /home/wadea
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.278 RHEL-09-411070 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

All RHEL 9 local interactive user home directories must be group-owned by the home directory owner's primary group.

```
GROUP ID: V-258053
RULE ID: SV-258053r991589
```

Rationale:

If the Group Identifier (GID) of a local interactive users home directory is not the same as the primary GID of the user, this would allow unauthorized access to the users files, and users that share the same group may not be able to access files that they legitimately should.

Audit:

Verify the assigned home directory of all local interactive users is group-owned by that user's primary GID with the following command:
Note: This may miss local interactive users that have been assigned a privileged user identifier (UID). Evidence of interactive use may be obtained from a number of log files containing system logon information. The returned directory "/home/wadea" is used as an example.

```
$ sudo ls -ld $(awk -F: '($3>=1000)&&($7 !~ /nologin/){print $6}'
/etc/passwd)

drwxr-x--- 2 wadea admin 4096 Jun 5 12:41 wadea
```

Check the user's primary group with the following command:

```
$ sudo grep $(grep wadea /etc/passwd | awk -F: `{print $4}') /etc/group

admin:x:250:wadea,jonesj,jacksons
```

If the user home directory referenced in "/etc/passwd" is not group-owned by that user's primary GID, this is a finding.

Remediation:

Change the group owner of a local interactive user's home directory to the group found in "/etc/passwd". To change the group owner of a local interactive user's home directory, use the following command:
Note: The example will be for the user "wadea", who has a home directory of "/home/wadea", and has a primary group of users.

```
$ sudo chgrp users /home/wadea
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.279 RHEL-09-411075 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must automatically lock an account when three unsuccessful logon attempts occur.

```
GROUP ID: V-258054
RULE ID: SV-258054r958736
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-force attacks, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005

Audit:

Verify RHEL 9 is configured to lock an account after three unsuccessful logon attempts with the command:

```
$ grep 'deny =' /etc/security/faillock.conf

deny = 3
```

If the "deny" option is not set to "3" or less (but not "0"), is missing or commented out, this is a finding.

Remediation:

Configure RHEL 9 to lock an account when three unsuccessful logon attempts occur. Add/modify the "/etc/security/faillock.conf" file to match the following line:

```
deny = 3
```

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53 :: AC-7 a
- NIST SP 800-53 Revision 4 :: AC-7 a
- NIST SP 800-53 Revision 5 :: AC-7 a
- NIST SP 800-53A :: AC-7.1 (ii)

CCI-002238 Automatically lock 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 logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4 :: AC-7 b
- NIST SP 800-53 Revision 5 :: AC-7 b

1.280 RHEL-09-411080 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must automatically lock the root account until the root account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.

```
GROUP ID: V-258055
RULE ID: SV-258055r1045140
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, also 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 RHEL 9 is configured to lock the root account after three unsuccessful logon attempts with the command:

```
$ sudo grep even_deny_root /etc/security/faillock.conf

even_deny_root
```

If the "even_deny_root" option is not set or is missing or commented out, this is a finding.

Remediation:

To configure RHEL 9 to lock out the "root" account after a number of incorrect logon attempts using "pam_faillock.so", first enable the feature using the following command:

```
$ sudo authselect enable-feature with-faillock
```

Edit the "/etc/security/faillock.conf" by uncommenting or adding the following line:

```
even_deny_root
```

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53 :: AC-7 a
- NIST SP 800-53 Revision 4 :: AC-7 a
- NIST SP 800-53 Revision 5 :: AC-7 a
- NIST SP 800-53A :: AC-7.1 (ii)

CCI-002238 Automatically lock 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 logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4 :: AC-7 b
- NIST SP 800-53 Revision 5 :: AC-7 b

1.281 RHEL-09-411085 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must automatically lock an account when three unsuccessful logon attempts occur during a 15-minute time period.

```
GROUP ID: V-258056
RULE ID: SV-258056r1045143
```

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:

Note: If the system administrator demonstrates the use of an approved centralized account management method that locks an account after three unsuccessful logon attempts within a period of 15 minutes, this requirement is Not Applicable.
Verify RHEL 9 locks an account after three unsuccessful logon attempts within a period of 15 minutes with the following command:

```
$ sudo grep fail_interval /etc/security/faillock.conf

fail_interval = 900
```

If the "fail_interval" option is not set to "900" or less (but not "0"), the line is commented out, or the line is missing, this is a finding.

Remediation:

To configure RHEL 9 to lock out the "root" account after a number of incorrect logon attempts within 15 minutes using "pam_faillock.so", enable the feature using the following command:

```
$ sudo authselect enable-feature with-faillock
```

Then edit the "/etc/security/faillock.conf" file as follows:

```
fail_interval = 900
```

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53 :: AC-7 a
- NIST SP 800-53 Revision 4 :: AC-7 a
- NIST SP 800-53 Revision 5 :: AC-7 a
- NIST SP 800-53A :: AC-7.1 (ii)

CCI-002238 Automatically lock 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 logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4 :: AC-7 b
- NIST SP 800-53 Revision 5 :: AC-7 b

1.282 RHEL-09-411090 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must maintain an account lock until the locked account is released by an administrator.

```
GROUP ID: V-258057
RULE ID: SV-258057r1045146
```

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 RHEL 9 is configured to lock an account until released by an administrator after three unsuccessful logon attempts with the command:

```
$ sudo grep -w unlock_time /etc/security/faillock.conf

unlock_time = 0
```

If the "unlock_time" option is not set to "0" or the line is missing or commented out, this is a finding.

Remediation:

Configure RHEL 9 to lock an account until released by an administrator after three unsuccessful logon attempts with the command:

```
$ sudo authselect enable-feature with-faillock
```

Edit the "/etc/security/faillock.conf" file as follows:

```
unlock_time = 0
```

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53 :: AC-7 a
- NIST SP 800-53 Revision 4 :: AC-7 a
- NIST SP 800-53 Revision 5 :: AC-7 a
- NIST SP 800-53A :: AC-7.1 (ii)

CCI-002238 Automatically lock 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 logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4 :: AC-7 b
- NIST SP 800-53 Revision 5 :: AC-7 b

1.283 RHEL-09-411095 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not have unauthorized accounts.

```
GROUP ID: V-258058
RULE ID: SV-258058r1045148
```

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 that there are no unauthorized interactive user accounts with the following command:

```
$ less /etc/passwd

root:x:0:0:root:/root:/bin/bash
...
games:x:12:100:games:/usr/games:/sbin/nologin
scsaustin:x:1001:1001:scsaustin:/home/scsaustin:/bin/bash
djohnson:x:1002:1002:djohnson:/home/djohnson:/bin/bash
```

Interactive user accounts generally will have a user identifier (UID) of 1000 or greater, a home directory in a specific partition, and an interactive shell.
Obtain the list of interactive user accounts authorized to be on the system from the system administrator or information system security officer (ISSO) and compare it to the list of local interactive user accounts on the system.
If there are unauthorized local user accounts on the system, this is a finding.

Remediation:

Remove unauthorized local interactive user accounts with the following command where <unauthorized_user> is the unauthorized account:

```
$ sudo userdel  <unauthorized_user>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.284 RHEL-09-411100 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

The root account must be the only account having unrestricted access to RHEL 9 system.

```
GROUP ID: V-258059
RULE ID: SV-258059r991589
```

Rationale:

An account has root authority if it has a user identifier (UID) of "0". Multiple accounts with a UID of "0" afford more opportunity for potential intruders to guess a password for a privileged account. Proper configuration of sudo is recommended to afford multiple system administrators access to root privileges in an accountable manner.

Audit:

Verify that only the "root" account has a UID "0" assignment with the following command:

```
$ awk -F: '$3 == 0 {print $1}' /etc/passwd

root
```

If any accounts other than "root" have a UID of "0", this is a finding.

Remediation:

Change the UID of any account on the system, other than root, that has a UID of "0". If the account is associated with system commands or applications, the UID should be changed to one greater than "0" but less than "1000". Otherwise, assign a UID of greater than "1000" that has not already been assigned.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.285 RHEL-09-411105 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must ensure account lockouts persist.

```
GROUP ID: V-258060
RULE ID: SV-258060r1045150
```

Rationale:

Having lockouts persist across reboots ensures that account is only unlocked by an administrator. If the lockouts did not persist across reboots, an attacker could simply reboot the system to continue brute force attacks against the accounts on the system.

Audit:

Verify the "/etc/security/faillock.conf" file is configured to use a nondefault faillock directory to ensure contents persist after reboot with the following command:

```
$ sudo grep -w dir /etc/security/faillock.conf

dir = /var/log/faillock
```

If the "dir" option is not set to a nondefault documented tally log directory or is missing or commented out, this is a finding.

Remediation:

Configure RHEL 9 maintain the contents of the faillock directory after a reboot. Add/modify the "/etc/security/faillock.conf" file to match the following line:

```
dir = /var/log/faillock
```

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53 :: AC-7 a
- NIST SP 800-53 Revision 4 :: AC-7 a
- NIST SP 800-53 Revision 5 :: AC-7 a
- NIST SP 800-53A :: AC-7.1 (ii)

1.286 RHEL-09-411110 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 groups must have unique Group ID (GID).

```
GROUP ID: V-258061
RULE ID: SV-258061r958482
```

Rationale:

To ensure accountability and prevent unauthenticated access, groups must be identified uniquely to prevent potential misuse and compromise of the system.

Audit:

Verify that RHEL 9 contains no duplicate GIDs for interactive users with the following command:

```
 $  cut -d : -f 3 /etc/group | uniq -d
```

If the system has duplicate GIDs, this is a finding.

Remediation:

Edit the file "/etc/group" and provide each group that has a duplicate GID with a unique GID.

Additional Information:

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53 :: IA-2
- NIST SP 800-53 Revision 4 :: IA-2
- NIST SP 800-53 Revision 5 :: IA-2
- NIST SP 800-53A :: IA-2.1

1.287 RHEL-09-411115 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Local RHEL 9 initialization files must not execute world-writable programs.

```
GROUP ID: V-258062
RULE ID: SV-258062r991589
```

Rationale:

If user start-up files execute world-writable programs, especially in unprotected directories, they could be maliciously modified to destroy user files or otherwise compromise the system at the user level. If the system is compromised at the user level, it is easier to elevate privileges to eventually compromise the system at the root and network level.

Audit:

Verify that local initialization files do not execute world-writable programs with the following command:
Note: The example will be for a system that is configured to create user home directories in the "/home" directory.

```
$ sudo find /home -perm -002 -type f -name ".[^.]*" -exec ls -ld {} \;
```

If any local initialization files are found to reference world-writable files, this is a finding.

Remediation:

Set the mode on files being executed by the local initialization files with the following command:

```
$ sudo chmod 0755 <file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.288 RHEL-09-412035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must automatically exit interactive command shell user sessions after 10 minutes of inactivity.

```
GROUP ID: V-258068
RULE ID: SV-258068r1069388
```

Rationale:

Terminating an idle interactive command shell user session within a short time period reduces the window of opportunity for unauthorized personnel to take control of it when left unattended in a virtual terminal or physical console.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000029-GPOS-00010

Audit:

Verify RHEL 9 is configured to exit interactive command shell user sessions after 10 minutes of inactivity or less with the following command:

```
$ sudo grep -i tmout /etc/profile /etc/profile.d/*.sh

/etc/profile.d/tmout.sh:declare -xr TMOUT=600
```

If "TMOUT" is not set to "600" or less in a script located in the "/etc/'profile.d/ directory, is missing or is commented out, this is a finding.

Remediation:

Configure RHEL 9 to exit interactive command shell user sessions after 10 minutes of inactivity.
Add or edit the following line in "/etc/profile.d/tmout.sh":

```
#!/bin/bash

declare -xr TMOUT=600
```

Additional Information:

CCI-000057 The information system initiates a session lock after the organization-defined time period of inactivity.

- NIST SP 800-53 :: AC-11 a
- NIST SP 800-53 Revision 4 :: AC-11 a
- NIST SP 800-53 Revision 5 :: AC-11 a
- NIST SP 800-53A :: AC-11.1 (ii)

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53 :: SC-10
- NIST SP 800-53 Revision 4 :: SC-10
- NIST SP 800-53 Revision 5 :: SC-10
- NIST SP 800-53A :: SC-10.1 (ii)

1.289 RHEL-09-412040 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

RHEL 9 must limit the number of concurrent sessions to ten for all accounts and/or account types.

```
GROUP ID: V-258069
RULE ID: SV-258069r958398
```

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 denial-of-service (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 must be defined based on mission needs and the operational environment for each system.

Audit:

Verify RHEL 9 limits the number of concurrent sessions to "10" for all accounts and/or account types with the following command:

```
$ grep -r -s maxlogins /etc/security/limits.conf
/etc/security/limits.d/*.conf

/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 set greater than "10" and is not documented with the information system security officer (ISSO) as an operational requirement for all domains that have the "maxlogins" item assigned, this is a finding.

Remediation:

Configure RHEL 9 to limit the number of concurrent sessions to "10" for all accounts and/or account types.
Add the following line to the top of the /etc/security/limits.conf or in a ".conf" file defined in /etc/security/limits.d/:

```
* hard maxlogins 10
```

Additional Information:

CCI-000054 Limit the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number.

- NIST SP 800-53 :: AC-10
- NIST SP 800-53 Revision 4 :: AC-10
- NIST SP 800-53 Revision 5 :: AC-10
- NIST SP 800-53A :: AC-10.1 (ii)

1.290 RHEL-09-412045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must log username information when unsuccessful logon attempts occur.

```
GROUP ID: V-258070
RULE ID: SV-258070r1045153
```

Rationale:

Without auditing of these events, it may be harder or impossible to identify what an attacker did after an attack.

Audit:

Verify the "/etc/security/faillock.conf" file is configured to log username information when unsuccessful logon attempts occur with the following command:

```
$ sudo grep audit /etc/security/faillock.conf

audit
```

If the "audit" option is not set, is missing, or is commented out, this is a finding.

Remediation:

Configure RHEL 9 to log username information when unsuccessful logon attempts occur.
Enable the feature using the following command:

```
$ sudo authselect enable-feature with-faillock
```

Add/modify the "/etc/security/faillock.conf" file to match the following line:

```
audit
```

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53 :: AC-7 a
- NIST SP 800-53 Revision 4 :: AC-7 a
- NIST SP 800-53 Revision 5 :: AC-7 a
- NIST SP 800-53A :: AC-7.1 (ii)

1.291 RHEL-09-412050 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must enforce a delay of at least four seconds between logon prompts following a failed logon attempt.

```
GROUP ID: V-258071
RULE ID: SV-258071r991588
```

Rationale:

Increasing the time between a failed authentication attempt and reprompting to enter credentials helps to slow a single-threaded brute force attack.

Audit:

Verify RHEL 9 enforces a delay of at least four seconds between console logon prompts following a failed logon attempt with the following command:

```
$ grep -i fail_delay /etc/login.defs

FAIL_DELAY 4
```

If the value of "FAIL_DELAY" is not set to "4" or greater, or the line is commented out, this is a finding.

Remediation:

Configure the RHEL 9 to enforce a delay of at least four seconds between logon prompts following a failed console logon attempt.
Modify the "/etc/login.defs" file to set the "FAIL_DELAY" parameter to 4 or greater:

```
FAIL_DELAY 4
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.292 RHEL-09-412055 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must define default permissions for the bash shell.

```
GROUP ID: V-258072
RULE ID: SV-258072r1045155
```

Rationale:

The umask controls the default access mode assigned to newly created files. A umask of 077 limits new files to mode 600 or less permissive. Although umask can be represented as a four-digit number, the first digit representing special access modes is typically ignored or required to be "0". This requirement applies to the globally configured system defaults and the local interactive user defaults for each account on the system.

Satisfies: SRG-OS-000480-GPOS-00228, SRG-OS-000480-GPOS-00227

Audit:

Verify the "umask" setting is configured correctly in the "/etc/bashrc" file with the following command:
Note: If the value of the "umask" parameter is set to "000" "/etc/bashrc" file, the Severity is raised to a CAT I.

```
$ grep umask /etc/bashrc

[ `umask` -eq 0 ] && umask 077
```

If the value for the "umask" parameter is not "077", or the "umask" parameter is missing or is commented out, this is a finding.

Remediation:

Configure RHEL 9 to define default permissions for all authenticated users using the bash shell.
Add or edit the lines for the "umask" parameter in the "/etc/bashrc" file to "077":

```
umask 077
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.293 RHEL-09-412060 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must define default permissions for the c shell.

```
GROUP ID: V-258073
RULE ID: SV-258073r1045157
```

Rationale:

The umask controls the default access mode assigned to newly created files. A umask of 077 limits new files to mode 600 or less permissive. Although umask can be represented as a four-digit number, the first digit representing special access modes is typically ignored or required to be "0". This requirement applies to the globally configured system defaults and the local interactive user defaults for each account on the system.

Satisfies: SRG-OS-000480-GPOS-00228, SRG-OS-000480-GPOS-00227

Audit:

Verify the "umask" setting is configured correctly in the "/etc/csh.cshrc" file with the following command:
Note: If the value of the "umask" parameter is set to "000" "/etc/csh.cshrc" file, the Severity is raised to a CAT I.

```
$ grep umask /etc/csh.cshrc

umask 077
```

If the value for the "umask" parameter is not "077", or the "umask" parameter is missing or is commented out, this is a finding.

Remediation:

Configure RHEL 9 to define default permissions for all authenticated users using the c shell.
Add or edit the lines for the "umask" parameter in the "/etc/csh.cshrc" file to "077":

```
umask 077
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.294 RHEL-09-412065 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must define default permissions for all authenticated users in such a way that the user can only read and modify their own files.

```
GROUP ID: V-258074
RULE ID: SV-258074r991590
```

Rationale:

Setting the most restrictive default permissions ensures that when new accounts are created, they do not have unnecessary access.

Audit:

Verify RHEL 9 defines default permissions for all authenticated users in such a way that the user can only read and modify their own files with the following command:
Note: If the value of the "UMASK" parameter is set to "000" in "/etc/login.defs" file, the Severity is raised to a CAT I.

```
# grep -i umask /etc/login.defs

UMASK 077
```

If the value for the "UMASK" parameter is not "077", or the "UMASK" parameter is missing or is commented out, this is a finding.

Remediation:

Configure RHEL 9 to define default permissions for all authenticated users in such a way that the user can only read and modify their own files.
Add or edit the lines for the "UMASK" parameter in the "/etc/login.defs" file to "077":

```
UMASK 077
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.295 RHEL-09-412070 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must define default permissions for the system default profile.

```
GROUP ID: V-258075
RULE ID: SV-258075r991590
```

Rationale:

The umask controls the default access mode assigned to newly created files. A umask of 077 limits new files to mode 600 or less permissive. Although umask can be represented as a four-digit number, the first digit representing special access modes is typically ignored or required to be "0". This requirement applies to the globally configured system defaults and the local interactive user defaults for each account on the system.

Satisfies: SRG-OS-000480-GPOS-00228, SRG-OS-000480-GPOS-00227

Audit:

Verify the "umask" setting is configured correctly in the "/etc/profile" file with the following command:
Note: If the value of the "umask" parameter is set to "000" "/etc/profile" file, the Severity is raised to a CAT I.

```
$ grep umask /etc/profile

umask 077
```

If the value for the "umask" parameter is not "077", or the "umask" parameter is missing or is commented out, this is a finding.

Remediation:

Configure RHEL 9 to define default permissions for all authenticated users in such a way that the user can only read and modify their own files.
Add or edit the lines for the "umask" parameter in the "/etc/profile" file to "077":

```
umask 077
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.296 RHEL-09-412075 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

RHEL 9 must display the date and time of the last successful account logon upon logon.

```
GROUP ID: V-258076
RULE ID: SV-258076r991589
```

Rationale:

Users need to be aware of activity that occurs regarding their account. Providing users with information regarding the number of unsuccessful attempts that were made to login to their account allows the user to determine if any unauthorized activity has occurred and gives them an opportunity to notify administrators.

Audit:

Verify users are provided with feedback on when account accesses last occurred with the following command:

```
$ sudo grep pam_lastlog /etc/pam.d/postlogin

session required pam_lastlog.so showfailed
```

If "pam_lastlog" is missing from "/etc/pam.d/postlogin" file, or the silent option is present, this is a finding.

Remediation:

Configure RHEL 9 to provide users with feedback on when account accesses last occurred by setting the required configuration options in "/etc/pam.d/postlogin".
Add the following line to the top of "/etc/pam.d/postlogin":

```
session required pam_lastlog.so showfailed
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.297 RHEL-09-412080 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must terminate idle user sessions.

```
GROUP ID: V-258077
RULE ID: SV-258077r1014874
```

Rationale:

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended.

Audit:

Verify that RHEL 9 logs out sessions that are idle for 15 minutes with the following command:

```
$ sudo grep -i ^StopIdleSessionSec /etc/systemd/logind.conf

StopIdleSessionSec=900
```

If "StopIdleSessionSec" is not configured to "900" seconds, this is a finding.

Remediation:

Configure RHEL 9 to log out idle sessions by editing the /etc/systemd/logind.conf file with the following line:

```
StopIdleSessionSec=900
```

The "logind" service must be restarted for the changes to take effect. To restart the "logind" service, run the following command:

```
$ sudo systemctl restart systemd-logind
```

Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53 :: SC-10
- NIST SP 800-53 Revision 4 :: SC-10
- NIST SP 800-53 Revision 5 :: SC-10
- NIST SP 800-53A :: SC-10.1 (ii)

1.298 RHEL-09-431010 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

RHEL 9 must use a Linux Security Module configured to enforce limits on system services.

```
GROUP ID: V-258078
RULE ID: SV-258078r958944
```

Rationale:

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

Satisfies: SRG-OS-000445-GPOS-00199, SRG-OS-000134-GPOS-00068

Audit:

Ensure that RHEL 9 verifies correct operation of security functions through the use of SELinux with the following command:

```
$ getenforce

Enforcing
```

If SELINUX is not set to "Enforcing", this is a finding.
Verify that SELinux is configured to be enforcing at boot.

```
grep "SELINUX=" /etc/selinux/config
# SELINUX= can take one of these three values:
# NOTE: In earlier Fedora kernel builds, SELINUX=disabled would also
SELINUX=enforcing
```

If SELINUX line is missing, commented out, or not set to "enforcing", this is a finding.

Remediation:

Configure RHEL 9 to verify correct operation of security functions.
Edit the file "/etc/selinux/config" and add or modify the following line:

```
SELINUX=enforcing
```

A reboot is required for the changes to take effect.

Additional Information:

CCI-001084 Isolate security functions from nonsecurity functions.

- NIST SP 800-53 :: SC-3
- NIST SP 800-53 Revision 4 :: SC-3
- NIST SP 800-53 Revision 5 :: SC-3
- NIST SP 800-53A :: SC-3.1 (ii)

CCI-002696 Verify correct operation of organization-defined security functions.

- NIST SP 800-53 Revision 4 :: SI-6 a
- NIST SP 800-53 Revision 5 :: SI-6 a

1.299 RHEL-09-431015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must enable the SELinux targeted policy.

```
GROUP ID: V-258079
RULE ID: SV-258079r1045159
```

Rationale:

Setting the SELinux policy to "targeted" or a more specialized policy ensures the system will confine processes that are likely to be targeted for exploitation, such as network or system services.

Note: During the development or debugging of SELinux modules, it is common to temporarily place nonproduction systems in "permissive" mode. In such temporary cases, SELinux policies should be developed, and once work is completed, the system should be reconfigured to "targeted".

Audit:

Verify the SELINUX on RHEL 9 is using the targeted policy with the following command:

```
$ sestatus | grep "policy name"

Loaded policy name:             targeted
```

If the loaded policy name is not "targeted", this is a finding.

Remediation:

Configure RHEL 9 to use the targetd SELINUX policy.
Edit the file "/etc/selinux/config" and add or modify the following line:

```
 SELINUXTYPE=targeted
```

A reboot is required for the changes to take effect.

Additional Information:

CCI-002696 Verify correct operation of organization-defined security functions.

- NIST SP 800-53 Revision 4 :: SI-6 a
- NIST SP 800-53 Revision 5 :: SI-6 a

1.300 RHEL-09-431016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must elevate the SELinux context when an administrator calls the sudo command.

```
GROUP ID: V-272496
RULE ID: SV-272496r1082184
```

Rationale:

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

Preventing nonprivileged 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. Nonprivileged users are individuals who do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from nonprivileged users.

Audit:

Verify that RHEL 9 elevates the SELinux context when an administrator calls the sudo command with the following command:
This command must be run as root:

```
# grep -r sysadm_r /etc/sudoers /etc/sudoers.d

%{designated_group_or_user_name} ALL=(ALL) TYPE=sysadm_t ROLE=sysadm_r ALL
```

If conflicting results are returned, this is a finding.
If a designated sudoers administrator group or account(s) is not configured to elevate the SELinux type and role to "sysadm_t" and "sysadm_r" with the use of the sudo command, this is a finding.

Remediation:

Configure RHEL 9 to elevate the SELinux context when an administrator calls the sudo command.
Edit a file in the "/etc/sudoers.d" directory with the following command:

```
$ sudo visudo -f /etc/sudoers.d/<customfile>
```

Use the following example to build the in the /etc/sudoers.d directory to allow any administrator belonging to a designated sudoers admin group to elevate their SELinux context with the use of the sudo command:

```
%{designated_group_or_user_name} ALL=(ALL) TYPE=sysadm_t ROLE=sysadm_r ALL
```

Remove any configurations that conflict with the above from the following locations:

```
/etc/sudoers
/etc/sudoers.d/
```

Additional Information:

CCI-002235 Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.301 RHEL-09-431020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must configure SELinux context type to allow the use of a nondefault faillock tally directory.

```
GROUP ID: V-258080
RULE ID: SV-258080r1045162
```

Rationale:

Not having the correct SELinux context on the faillock directory may lead to unauthorized access to the directory.

Audit:

Verify the location of the nondefault tally directory for the pam_faillock module with the following command:
Note: If the system does not have SELinux enabled and enforcing a targeted policy, or if the pam_faillock module is not configured for use, this requirement is Not Applicable.

```
$ sudo grep -w dir /etc/security/faillock.conf

dir = /var/log/faillock
```

Check the security context type of the nondefault tally directory with the following command:

```
$ ls -Zd /var/log/faillock

unconfined_u:object_r:faillog_t:s0 /var/log/faillock
```

If the security context type of the nondefault tally directory is not "faillog_t", this is a finding.

Remediation:

Configure RHEL 9 to allow the use of a nondefault faillock tally directory while SELinux enforces a targeted policy.
First enable the feature using the following command:

```
$ sudo authselect enable-feature with-faillock
```

Create a nondefault faillock tally directory (if it does not already exist) with the following example:

```
$ sudo mkdir /var/log/faillock
```

Then add/modify the "/etc/security/faillock.conf" file to match the following line:

```
dir = /var/log/faillock
```

Update the /etc/selinux/targeted/contexts/files/file_contexts.local with "faillog_t" context type for the nondefault faillock tally directory with the following command:

```
$ sudo semanage fcontext -a -t faillog_t "/var/log/faillock(/.*)?"
```

Next, update the context type of the nondefault faillock directory/subdirectories and files with the following command:

```
$ sudo restorecon -R -v /var/log/faillock
```

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53 :: AC-7 a
- NIST SP 800-53 Revision 4 :: AC-7 a
- NIST SP 800-53 Revision 5 :: AC-7 a
- NIST SP 800-53A :: AC-7.1 (ii)

1.302 RHEL-09-431025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must have policycoreutils package installed.

```
GROUP ID: V-258081
RULE ID: SV-258081r1045164
```

Rationale:

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

Policycoreutils contains the policy core utilities that are required for basic operation of an SELinux-enabled system. These utilities include load_policy to load SELinux policies, setfile to label filesystems, newrole to switch roles, and run_init to run /etc/init.d scripts in the proper context.

Satisfies: SRG-OS-000480-GPOS-00227, SRG-OS-000134-GPOS-00068

Audit:

Verify RHEL 9 has the policycoreutils package installed with the following command:

```
$ dnf list --installed policycoreutils
```

Example output:

```
policycoreutils.x86_64          3.3-6.el9_0
```

If the "policycoreutils" package is not installed, this is a finding.

Remediation:

The policycoreutils package can be installed with the following command:

```
$ sudo dnf install policycoreutils
```

Additional Information:

CCI-001084 Isolate security functions from nonsecurity functions.

- NIST SP 800-53 :: SC-3
- NIST SP 800-53 Revision 4 :: SC-3
- NIST SP 800-53 Revision 5 :: SC-3
- NIST SP 800-53A :: SC-3.1 (ii)

1.303 RHEL-09-431030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 policycoreutils-python-utils package must be installed.

```
GROUP ID: V-258082
RULE ID: SV-258082r1045166
```

Rationale:

The policycoreutils-python-utils package is required to operate and manage an SELinux environment and its policies. It provides utilities such as semanage, audit2allow, audit2why, chcat, and sandbox.

Audit:

Verify that RHEL 9 policycoreutils-python-utils service package is installed with the following command:

```
$ dnf list --installed policycoreutils-python-utils
```

Example output:

```
policycoreutils-python-utils.noarch          3.3-6.el9_0
```

If the "policycoreutils-python-utils" package is not installed, this is a finding.

Remediation:

Install the policycoreutils-python-utils service package (if the policycoreutils-python-utils service is not already installed) with the following command:

```
$ sudo dnf install policycoreutils-python-utils
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.304 RHEL-09-432010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must have the sudo package installed.

```
GROUP ID: V-258083
RULE ID: SV-258083r1045168
```

Rationale:

"sudo" is a program designed to allow a system administrator to give limited root privileges to users and log root activity. The basic philosophy is to give as few privileges as possible but still allow system users to get their work done.

Audit:

Verify that RHEL 9 sudo package is installed with the following command:

```
$ dnf list --installed sudo
```

Example output:

```
sudo.x86_64          1.9.5p2-7.el9
```

If the "sudo" package is not installed, this is a finding.

Remediation:

The sudo package can be installed with the following command:

```
$ sudo dnf install sudo
```

Additional Information:

CCI-002235 Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (10)
- NIST SP 800-53 Revision 5 :: AC-6 (10)

1.305 RHEL-09-432015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must require reauthentication when using the "sudo" command.

```
GROUP ID: V-258084
RULE ID: SV-258084r1050789
```

Rationale:

Without reauthentication, 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 reauthenticate 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 reauthenticate for privileged actions until the user's session is terminated.

Audit:

Verify RHEL 9 requires reauthentication when using the "sudo" command to elevate privileges with the following command:

```
$ sudo grep -ir 'timestamp_timeout' /etc/sudoers /etc/sudoers.d/

/etc/sudoers:Defaults timestamp_timeout=0
```

If results are returned from more than one file location, this is a finding.
If "timestamp_timeout" is set to a negative number, is commented out, or no results are returned, this is a finding.

Remediation:

Configure RHEL 9 to reauthenticate "sudo" commands after the specified timeout:
Add the following line to "/etc/sudoers" or a file in "/etc/sudoers.d":

```
Defaults timestamp_timeout=0
```

Additional Information:

CCI-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5 :: SC-11 b

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4 :: IA-11

1.306 RHEL-09-432020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must use the invoking user's password for privilege escalation when using "sudo".

```
GROUP ID: V-258085
RULE ID: SV-258085r1045173
```

Rationale:

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.

Audit:

Verify that the sudoers security policy is configured to use the invoking user's password for privilege escalation with the following command:

```
$ sudo egrep -ir '(!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 results are returned from more than one file location, 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 single configuration file in the /etc/sudoers.d/ directory:

```
Defaults !targetpw
Defaults !rootpw
Defaults !runaspw
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.307 RHEL-09-432025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must require users to reauthenticate for privilege escalation.

```
GROUP ID: V-258086
RULE ID: SV-258086r1050789
```

Rationale:

Without reauthentication, 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 that the user reauthenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Audit:

Verify that "/etc/sudoers" has no occurrences of "!authenticate" with the following command:

```
$ sudo grep -ir '!authenticate' /etc/sudoers /etc/sudoers.d/
```

If any occurrences of "!authenticate" are returned, this is a finding.

Remediation:

Configure RHEL 9 to not allow users to execute privileged actions without authenticating.
Remove any occurrence of "!authenticate" found in "/etc/sudoers" file or files in the "/etc/sudoers.d" directory.

```
$ sudo sed -i '/\!authenticate/ s/^/# /g' /etc/sudoers /etc/sudoers.d/*
```

Additional Information:

CCI-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5 :: SC-11 b

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4 :: IA-11

1.308 RHEL-09-432030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must restrict privilege elevation to authorized personnel.

```
GROUP ID: V-258087
RULE ID: SV-258087r1045177
```

Rationale:

If the "sudoers" file is not configured correctly, any user defined on the system can initiate privileged actions on the target system.

Audit:

Verify RHEL 9 restricts privilege elevation to authorized personnel with the following command:

```
$ sudo grep -riw 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 /etc/sudoers file or configuration file under /etc/sudoers.d/:

```
ALL     ALL=(ALL) ALL
ALL     ALL=(ALL:ALL) ALL
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.309 RHEL-09-432035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must restrict the use of the "su" command.

```
GROUP ID: V-258088
RULE ID: SV-258088r1050789
```

Rationale:

The "su" program allows to run commands with a substitute user and group ID. It is commonly used to run commands as the root user. Limiting access to such commands is considered a good security practice.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000312-GPOS-00123

Audit:

Verify that RHEL 9 requires uses to be members of the "wheel" group with the following command:

```
$ grep pam_wheel /etc/pam.d/su

auth             required        pam_wheel.so use_uid
```

If a line for "pam_wheel.so" does not exist, or is commented out, this is a finding.

Remediation:

Configure RHEL 9 to require users to be in the "wheel" group to run "su" command.
In file "/etc/pam.d/su", uncomment the following line:
"#auth required pam_wheel.so use_uid"

```
$ sed
'/^[[:space:]]*#[[:space:]]*auth[[:space:]]\+required[[:space:]]\+pam_wheel\.
so[[:space:]]\+use_uid$/s/^[[:space:]]*#//' -i /etc/pam.d/su
```

If necessary, create a "wheel" group and add administrative users to the group.

Additional Information:

CCI-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5 :: SC-11 b

CCI-002165 Enforce organization-defined discretionary access control policies over defined subjects and objects.

- NIST SP 800-53 Revision 4 :: AC-3 (4)
- NIST SP 800-53 Revision 5 :: AC-3 (4)

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4 :: IA-11

1.310 RHEL-09-433010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 fapolicy module must be installed.

```
GROUP ID: V-258089
RULE ID: SV-258089r1045179
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as allow listing.

Utilizing an allow list provides a configuration management method for allowing the execution of only authorized software. Using only authorized software decreases risk by limiting the number of potential vulnerabilities. Verification of allow listed software occurs prior to execution or at system startup.

User home directories/folders may contain information of a sensitive nature. Nonprivileged users should coordinate any sharing of information with an SA through shared resources.

RHEL 9 ships with many optional packages. One such package is a file access policy daemon called "fapolicyd". "fapolicyd" is a userspace daemon that determines access rights to files based on attributes of the process and file. It can be used to either blocklist or allow list processes or file access.

Proceed with caution with enforcing the use of this daemon. Improper configuration may render the system nonfunctional. The "fapolicyd" API is not namespace aware and can cause issues when launching or running containers.

Satisfies: SRG-OS-000370-GPOS-00155, SRG-OS-000368-GPOS-00154

Audit:

Verify that RHEL 9 fapolicyd package is installed with the following command:

```
$ dnf list --installed fapolicyd
```

Example output:

```
fapolicyd.x86_64          1.1-103.el9_0
```

If the "fapolicyd" package is not installed, this is a finding.

Remediation:

The fapolicyd package can be installed with the following command:

```
$ sudo dnf install fapolicyd
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

CCI-001774 Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system.

- NIST SP 800-53 Revision 4 :: CM-7 (5) (b)
- NIST SP 800-53 Revision 5 :: CM-7 (5) (b)

1.311 RHEL-09-433015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 fapolicy module must be enabled.

```
GROUP ID: V-258090
RULE ID: SV-258090r958808
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as allowlisting.

Utilizing an allowlist provides a configuration management method for allowing the execution of only authorized software. Using only authorized software decreases risk by limiting the number of potential vulnerabilities. Verification of allowlisted software occurs prior to execution or at system startup.

User home directories/folders may contain information of a sensitive nature. Nonprivileged users should coordinate any sharing of information with an SA through shared resources.

RHEL 9 ships with many optional packages. One such package is a file access policy daemon called "fapolicyd". "fapolicyd" is a userspace daemon that determines access rights to files based on attributes of the process and file. It can be used to either blocklist or allowlist processes or file access.

Proceed with caution with enforcing the use of this daemon. Improper configuration may render the system nonfunctional. The "fapolicyd" API is not namespace aware and can cause issues when launching or running containers.

Satisfies: SRG-OS-000370-GPOS-00155, SRG-OS-000368-GPOS-00154

Audit:

Verify that RHEL 9 fapolicyd is active with the following command:

```
$ systemctl is-active fapolicyd

active
```

If fapolicyd module is not active, this is a finding.

Remediation:

Enable the fapolicyd with the following command:

```
$ systemctl enable --now fapolicyd
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

CCI-001774 Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system.

- NIST SP 800-53 Revision 4 :: CM-7 (5) (b)
- NIST SP 800-53 Revision 5 :: CM-7 (5) (b)

1.312 RHEL-09-433016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The RHEL 9 fapolicy module must be configured to employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs.

```
GROUP ID: V-270180
RULE ID: SV-270180r1045182
```

Rationale:

The organization must identify authorized software programs and permit execution of authorized software. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as allow listing.

Using an allow list provides a configuration management method for allowing the execution of only authorized software. Using only authorized software decreases risk by limiting the number of potential vulnerabilities. Verification of allow listed software occurs prior to execution or at system startup.

User home directories/folders may contain information of a sensitive nature. Nonprivileged users should coordinate any sharing of information with an SA through shared resources.

RHEL 9 ships with many optional packages. One such package is a file access policy daemon called "fapolicyd". "fapolicyd" is a userspace daemon that determines access rights to files based on attributes of the process and file. It can be used to either block list or allow list processes or file access.

Proceed with caution with enforcing the use of this daemon. Improper configuration may render the system nonfunctional. The "fapolicyd" API is not namespace aware and can cause issues when launching or running containers.

Satisfies: SRG-OS-000368-GPOS-00154, SRG-OS-000370-GPOS-00155, SRG-OS-000480-GPOS-00232

Audit:

Verify the RHEL 9 "fapolicyd" employs a deny-all, permit-by-exception policy.
Check that "fapolicyd" is in enforcement mode with the following command:

```
$ sudo grep permissive /etc/fapolicyd/fapolicyd.conf

permissive = 0
```

Check that "fapolicyd" employs a deny-all policy on system mounts with the following commands:

```
$ sudo tail /etc/fapolicyd/compiled.rules

allow exe=/usr/bin/python3.7 : ftype=text/x-python
deny_audit perm=any pattern=ld_so : all
deny perm=any all : all
```

If "fapolicyd" is not running in enforcement mode with a deny-all, permit-by-exception policy, this is a finding.

Remediation:

Configure RHEL 9 to employ a deny-all, permit-by-exception application allow listing policy with "fapolicyd".
With the "fapolicyd" installed and enabled, configure the daemon to function in permissive mode until the allow list is built correctly to avoid system lockout. Do this by editing the "/etc/fapolicyd/fapolicyd.conf" file with the following line:

```
permissive = 1
```

Build the allow list in a file within the "/etc/fapolicyd/rules.d" directory, ensuring the last rule is "deny perm=any all : all".
Once it is determined the allow list is built correctly, set the "fapolicyd" to enforcing mode by editing the "permissive" line in the /etc/fapolicyd/fapolicyd.conf file.

```
permissive = 0
```

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4 :: CM-7 (2)
- NIST SP 800-53 Revision 5 :: CM-7 (2)

1.313 RHEL-09-611010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must ensure the password complexity module in the system-auth file is configured for three retries or less.

```
GROUP ID: V-258091
RULE ID: SV-258091r1045185
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. "pwquality" enforces complex password construction configuration and has the ability to limit brute-force attacks on the system.

RHEL 9 uses "pwquality" as a mechanism to enforce password complexity. This is set in both: /etc/pam.d/password-auth /etc/pam.d/system-auth

By limiting the number of attempts to meet the pwquality module complexity requirements before returning with an error, the system will audit abnormal attempts at password changes.

Audit:

Verify RHEL 9 is configured to limit the "pwquality" retry option to "3".
Check for the use of the retry option in the security directory with the following command:

```
$ grep -w retry /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf

retry = 3
```

If the value of "retry" is set to "0" or greater than "3", or is missing, this is a finding.

Remediation:

Configure RHEL 9 to limit the "pwquality" retry option to "3".
Add or update the following line in the "/etc/security/pwquality.conf" file or a file in the "/etc/security/pwquality.conf.d/" directory to contain the "retry" parameter:

```
retry = 3
```

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000192 The information system enforces password complexity by the minimum number of upper case characters used.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.314 RHEL-09-611025 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

RHEL 9 must not allow blank or null passwords.

```
GROUP ID: V-258094
RULE ID: SV-258094r1045187
```

Rationale:

If an account has an empty password, anyone could log in and run commands with the privileges of that account. Accounts with empty passwords should never be used in operational environments.

Audit:

Verify that null passwords cannot be used with the following command:

```
$ sudo grep -i nullok /etc/pam.d/system-auth /etc/pam.d/password-auth
```

If output is produced, this is a finding.
If the system administrator (SA) can demonstrate that the required configuration is contained in a PAM configuration file included or substacked from the system-auth file, this is not a finding.

Remediation:

If PAM is managed with authselect, use the following command to remove instances of "nullok":

```
$ sudo authselect enable-feature without-nullok
```

Otherwise, remove any instances of the "nullok" option in the "/etc/pam.d/password-auth" and "/etc/pam.d/system-auth" files to prevent logons with empty passwords.
Note: Manual changes to the listed file may be overwritten by the "authselect" program.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.315 RHEL-09-611030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must configure the use of the pam_faillock.so module in the /etc/pam.d/system-auth file.

```
GROUP ID: V-258095
RULE ID: SV-258095r1045189
```

Rationale:

If the pam_faillock.so module is not loaded, the system will not correctly lockout accounts to prevent password guessing attacks.

Audit:

Verify the pam_faillock.so module is present in the "/etc/pam.d/system-auth" file:

```
$ grep pam_faillock.so /etc/pam.d/system-auth

auth required pam_faillock.so preauth
auth required pam_faillock.so authfail
account required pam_faillock.so
```

If the pam_faillock.so module is not present in the "/etc/pam.d/system-auth" file with the "preauth" line listed before pam_unix.so, this is a finding.
If the system administrator (SA) can demonstrate that the required configuration is contained in a PAM configuration file included or substacked from the system-auth file, this is not a finding.

Remediation:

Configure RHEL 9 to include the use of the pam_faillock.so module in the /etc/pam.d/system-auth file.
If PAM is managed with authselect, enable the feature with the following command:

```
$ sudo authselect enable-feature with-faillock
```

Otherwise, add/modify the appropriate sections of the "/etc/pam.d/system-auth" file to match the following lines:
Note: The "preauth" line must be listed before pam_unix.so.

```
auth required pam_faillock.so preauth
auth required pam_faillock.so authfail
account required pam_faillock.so
```

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53 :: AC-7 a
- NIST SP 800-53 Revision 4 :: AC-7 a
- NIST SP 800-53 Revision 5 :: AC-7 a
- NIST SP 800-53A :: AC-7.1 (ii)

1.316 RHEL-09-611035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must configure the use of the pam_faillock.so module in the /etc/pam.d/password-auth file.

```
GROUP ID: V-258096
RULE ID: SV-258096r1045191
```

Rationale:

If the pam_faillock.so module is not loaded, the system will not correctly lockout accounts to prevent password guessing attacks.

Audit:

Verify the pam_faillock.so module is present in the "/etc/pam.d/password-auth" file:

```
$ grep pam_faillock.so /etc/pam.d/password-auth

auth required pam_faillock.so preauth
auth required pam_faillock.so authfail
account required pam_faillock.so
```

If the pam_faillock.so module is not present in the "/etc/pam.d/password-auth" file with the "preauth" line listed before pam_unix.so, this is a finding.
If the system administrator (SA) can demonstrate that the required configuration is contained in a PAM configuration file included or substacked from the system-auth file, this is not a finding.

Remediation:

Configure RHEL 9 to include the use of the pam_faillock.so module in the /etc/pam.d/password-auth file. If PAM is managed with authselect, enable the feature with the following command:

```
$ sudo authselect enable-feature with-faillock
```

Otherwise, add/modify the appropriate sections of the "/etc/pam.d/password-auth" file to match the following lines:
Note: The "preauth" line must be listed before pam_unix.so.

```
auth required pam_faillock.so preauth
auth required pam_faillock.so authfail
account required pam_faillock.so
```

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53 :: AC-7 a
- NIST SP 800-53 Revision 4 :: AC-7 a
- NIST SP 800-53 Revision 5 :: AC-7 a
- NIST SP 800-53A :: AC-7.1 (ii)

1.317 RHEL-09-611040 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must ensure the password complexity module is enabled in the password-auth file.

```
GROUP ID: V-258097
RULE ID: SV-258097r1045193
```

Rationale:

Enabling PAM password complexity permits enforcement of strong passwords and consequently makes the system less prone to dictionary attacks.

Satisfies: SRG-OS-000069-GPOS-00037, SRG-OS-000070-GPOS-00038, SRG-OS-000480-GPOS-00227

Audit:

Verify RHEL 9 uses "pwquality" to enforce the password complexity rules in the password-auth file with the following command:

```
$ grep pam_pwquality /etc/pam.d/password-auth

password required pam_pwquality.so
```

If the command does not return a line containing the value "pam_pwquality.so", or the line is commented out, this is a finding.
If the system administrator (SA) can demonstrate that the required configuration is contained in a PAM configuration file included or substacked from the system-auth file, this is not a finding.

Remediation:

Configure RHEL 9 to use "pwquality" to enforce password complexity rules.
Add the following line to the "/etc/pam.d/password-auth" file (or modify the line to have the required value):

```
password required pam_pwquality.so
```

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000192 The information system enforces password complexity by the minimum number of upper case characters used.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (v)

CCI-000193 The information system enforces password complexity by the minimum number of lower case characters used.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.318 RHEL-09-611045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must ensure the password complexity module is enabled in the system-auth file.

```
GROUP ID: V-258098
RULE ID: SV-258098r1045195
```

Rationale:

Enabling PAM password complexity permits enforcement of strong passwords and consequently makes the system less prone to dictionary attacks.

Audit:

Verify RHEL 9 uses "pwquality" to enforce the password complexity rules in the system-auth file with the following command:

```
$ grep pam_pwquality /etc/pam.d/system-auth

password required pam_pwquality.so
```

If the command does not return a line containing the value "pam_pwquality.so", or the line is commented out, this is a finding.
If the system administrator (SA) can demonstrate that the required configuration is contained in a PAM configuration file included or substacked from the system-auth file, this is not a finding.

Remediation:

Configure RHEL 9 to use "pwquality" to enforce password complexity rules.
Add the following line to the "/etc/pam.d/system-auth" file(or modify the line to have the required value):

```
password required pam_pwquality.so
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.319 RHEL-09-611050 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 password-auth must be configured to use a sufficient number of hashing rounds.

```
GROUP ID: V-258099
RULE ID: SV-258099r1045198
```

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 that are encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Using more hashing rounds makes password cracking attacks more difficult.

Satisfies: SRG-OS-000073-GPOS-00041, SRG-OS-000120-GPOS-00061

Audit:

Verify the number of rounds for the password hashing algorithm is configured with the following command:

```
$ grep rounds /etc/pam.d/password-auth

password sufficient pam_unix.so sha512 rounds=100000
```

If a matching line is not returned or "rounds" is less than "100000", this a finding.

Remediation:

Configure RHEL 9 to use 100000 hashing rounds for hashing passwords.
Add or modify the following line in "/etc/pam.d/password-auth" and set "rounds" to "100000".

```
password sufficient pam_unix.so sha512 rounds=100000
```

Note: Running authselect will overwrite this value unless a custom authselect policy is created.

Additional Information:

CCI-004062 For password-based authentication, store passwords using an approved salted key derivation function, preferably using a keyed hash.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (d)

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53 :: IA-7
- NIST SP 800-53 Revision 4 :: IA-7
- NIST SP 800-53 Revision 5 :: IA-7
- NIST SP 800-53A :: IA-7.1

CCI-000196 The information system, for password-based authentication, stores only cryptographically-protected passwords.

- NIST SP 800-53 :: IA-5 (1) (c)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (c)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.320 RHEL-09-611055 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 system-auth must be configured to use a sufficient number of hashing rounds.

```
GROUP ID: V-258100
RULE ID: SV-258100r1045201
```

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 that are encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Using more hashing rounds makes password cracking attacks more difficult.

Satisfies: SRG-OS-000073-GPOS-00041, SRG-OS-000120-GPOS-00061

Audit:

Verify the number of rounds for the password hashing algorithm is configured with the following command:

```
$ sudo grep rounds /etc/pam.d/system-auth

password sufficient pam_unix.so sha512 rounds=100000
```

If a matching line is not returned or "rounds" is less than 100000, this a finding.

Remediation:

Configure RHEL 9 to use 100000 hashing rounds for hashing passwords.
Add or modify the following line in "/etc/pam.d/system-auth" and set "rounds" to 100000.

```
password sufficient pam_unix.so sha512 rounds=100000
```

Note: Running authselect will overwrite this value unless a custom authselect policy is created.

Additional Information:

CCI-004062 For password-based authentication, store passwords using an approved salted key derivation function, preferably using a keyed hash.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (d)

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53 :: IA-7
- NIST SP 800-53 Revision 4 :: IA-7
- NIST SP 800-53 Revision 5 :: IA-7
- NIST SP 800-53A :: IA-7.1

CCI-000196 The information system, for password-based authentication, stores only cryptographically-protected passwords.

- NIST SP 800-53 :: IA-5 (1) (c)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (c)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.321 RHEL-09-611060 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must enforce password complexity rules for the root account.

```
GROUP ID: V-258101
RULE ID: SV-258101r1045204
```

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.

Satisfies: SRG-OS-000072-GPOS-00040, SRG-OS-000071-GPOS-00039, SRG-OS-000070-GPOS-00038, SRG-OS-000266-GPOS-00101, SRG-OS-000078-GPOS-00046, SRG-OS-000480-GPOS-00225, SRG-OS-000069-GPOS-00037

Audit:

Verify that RHEL 9 enforces password complexity rules for the root account.
Check if root user is required to use complex passwords with the following command:

```
$ grep enforce_for_root /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf

/etc/security/pwquality.conf:enforce_for_root
```

If "enforce_for_root" is commented or missing, this is a finding.

Remediation:

Configure RHEL 9 to enforce password complexity on the root account.
Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory to contain the "enforce_for_root" parameter:

```
enforce_for_root
```

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000192 The information system enforces password complexity by the minimum number of upper case characters used.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (v)

CCI-000193 The information system enforces password complexity by the minimum number of lower case characters used.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (v)

CCI-000194 The information system enforces password complexity by the minimum number of numeric characters used.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (v)

CCI-000195 The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.

- NIST SP 800-53 :: IA-5 (1) (b)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (b)
- NIST SP 800-53A :: IA-5 (1).1 (v)

CCI-000205 The information system enforces minimum password length.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (i)

CCI-001619 The information system enforces password complexity by the minimum number of special characters used.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.322 RHEL-09-611065 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must enforce password complexity by requiring that at least one lowercase character be used.

```
GROUP ID: V-258102
RULE ID: SV-258102r1045207
```

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. Requiring a minimum number of lowercase characters makes password guessing attacks more difficult by ensuring a larger search space.

Audit:

Verify that RHEL 9 enforces password complexity by requiring at least one lowercase character.
Check the value for "lcredit" with the following command:

```
$ grep lcredit /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf

/etc/security/pwquality.conf:lcredit = -1
```

If the value of "lcredit" is a positive number or is commented out, this is a finding.

Remediation:

Configure RHEL 9 to enforce password complexity by requiring at least one lowercase character be used by setting the "lcredit" option.
Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory to contain the "lcredit" parameter:

```
lcredit = -1
```

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000193 The information system enforces password complexity by the minimum number of lower case characters used.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.323 RHEL-09-611070 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must enforce password complexity by requiring that at least one numeric character be used.

```
GROUP ID: V-258103
RULE ID: SV-258103r1045210
```

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. Requiring digits makes password guessing attacks more difficult by ensuring a larger search space.

Audit:

Verify that RHEL 9 enforces password complexity by requiring at least one numeric character.
Check the value for "dcredit" with the following command:

```
$ grep dcredit /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf

/etc/security/pwquality.conf:dcredit = -1
```

If the value of "dcredit" is a positive number or is commented out, this is a finding.

Remediation:

Configure RHEL 9 to enforce password complexity by requiring at least one numeric character be used by setting the "dcredit" option.
Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory to contain the "dcredit" parameter:

```
dcredit = -1
```

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

1. NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000194 The information system enforces password complexity by the minimum number of numeric characters used.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.324 RHEL-09-611075 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 passwords for new users or password changes must have a 24 hours minimum password lifetime restriction in /etc/login.defs.

```
GROUP ID: V-258104
RULE ID: SV-258104r1015104
```

Rationale:

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, then the password could be repeatedly changed in a short period of time to defeat the organization's policy regarding password reuse.

Setting the minimum password age protects against users cycling back to a favorite password after satisfying the password reuse requirement.

Audit:

Verify RHEL 9 enforces 24 hours as the minimum password lifetime for new user accounts.
Check for the value of "PASS_MIN_DAYS" in "/etc/login.defs" with the following command:

```
$ grep -i pass_min_days /etc/login.defs

PASS_MIN_DAYS 1
```

If the "PASS_MIN_DAYS" parameter value is not "1" or greater, or is commented out, this is a finding.

Remediation:

Configure RHEL 9 to enforce 24 hours as the minimum password lifetime.
Add the following line in "/etc/login.defs" (or modify the line to have the required value):

```
PASS_MIN_DAYS 1
```

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000198 The information system enforces minimum password lifetime restrictions.

- NIST SP 800-53 :: IA-5 (1) (d)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (d)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.325 RHEL-09-611080 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 passwords must have a 24 hours minimum password lifetime restriction in /etc/shadow.

```
GROUP ID: V-258105
RULE ID: SV-258105r1045212
```

Rationale:

Enforcing a minimum password lifetime helps to prevent repeated password changes to defeat the password reuse or history enforcement requirement. If users are allowed to immediately and continually change their password, the password could be repeatedly changed in a short period of time to defeat the organization's policy regarding password reuse.

Audit:

Verify that RHEL 9 has configured the minimum time period between password changes for each user account as one day or greater with the following command:

```
$ sudo awk -F: '$4 < 1 {printf "%s %d\n", $1, $4}' /etc/shadow
```

If any results are returned that are not associated with a system account, this is a finding.

Remediation:

Configure noncompliant accounts to enforce a 24 hour minimum password lifetime:

```
$ sudo passwd -n 1 [user]
```

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000198 The information system enforces minimum password lifetime restrictions.

- NIST SP 800-53 :: IA-5 (1) (d)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (d)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.326 RHEL-09-611085 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must require users to provide a password for privilege escalation.

```
GROUP ID: V-258106
RULE ID: SV-258106r1050789
```

Rationale:

Without reauthentication, 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 that the user reauthenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Audit:

Verify that "/etc/sudoers" has no occurrences of "NOPASSWD" with the following command:

```
$ sudo grep -ri nopasswd /etc/sudoers /etc/sudoers.d/
```

If any occurrences of "NOPASSWD" are returned from the command and have not been documented with the information system security officer (ISSO) as an organizationally defined administrative group using MFA, this is a finding.

Remediation:

Configure RHEL 9 to not allow users to execute privileged actions without authenticating with a password.
Remove any occurrence of "NOPASSWD" found in "/etc/sudoers" file or files in the "/etc/sudoers.d" directory.

```
$ sudo find /etc/sudoers /etc/sudoers.d -type f -exec sed -i '/NOPASSWD/
s/^/# /g' {} \;
```

Additional Information:

CCI-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5 :: SC-11 b

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4 :: IA-11

1.327 RHEL-09-611090 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 passwords must be created with a minimum of 15 characters.

```
GROUP ID: V-258107
RULE ID: SV-258107r1045218
```

Rationale:

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. Use of more characters in a password helps to increase exponentially the time and/or resources required to compromise the password.

RHEL 9 uses "pwquality" as a mechanism to enforce password complexity. Configurations are set in the "etc/security/pwquality.conf" file.

The "minlen", sometimes noted as minimum length, acts as a "score" of complexity based on the credit components of the "pwquality" module. By setting the credit components to a negative value, not only will those components be required, but they will not count toward the total "score" of "minlen". This will enable "minlen" to require a 15-character minimum.

The DOD minimum password requirement is 15 characters.

Audit:

Verify that RHEL 9 enforces a minimum 15-character password length with the following command:

```
$ grep minlen /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf

minlen = 15
```

If the command does not return a "minlen" value of "15" or greater, does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to enforce a minimum 15-character password length.
Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory to contain the "minlen" parameter:

```
minlen = 15
```

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000205 The information system enforces minimum password length.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (i)

1.328 RHEL-09-611100 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must enforce password complexity by requiring that at least one special character be used.

```
GROUP ID: V-258109
RULE ID: SV-258109r1045220
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised. RHEL 9 utilizes "pwquality" as a mechanism to enforce password complexity. Note that to require special characters without degrading the "minlen" value, the credit value must be expressed as a negative number in "/etc/security/pwquality.conf".

Audit:

Verify that RHEL 9 enforces password complexity by requiring at least one special character with the following command:

```
$ sudo grep ocredit /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf

ocredit = -1
```

If the value of "ocredit" is a positive number or is commented out, this is a finding.

Remediation:

Configure RHEL 9 to enforce password complexity by requiring at least one special character be used by setting the "ocredit" option.
Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory to contain the "ocredit" parameter:

```
ocredit = -1
```

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-001619 The information system enforces password complexity by the minimum number of special characters used.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.329 RHEL-09-611105 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prevent the use of dictionary words for passwords.

```
GROUP ID: V-258110
RULE ID: SV-258110r1045223
```

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. If RHEL 9 allows the user to select passwords based on dictionary words, this increases the chances of password compromise by increasing the opportunity for successful guesses, and brute-force attacks.

Audit:

Verify RHEL 9 prevents the use of dictionary words for passwords with the following command:

```
$ grep dictcheck /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf

/etc/security/pwquality.conf:dictcheck = 1
```

If "dictcheck" does not have a value other than "0", or is commented out, this is a finding.

Remediation:

Configure RHEL 9 to prevent the use of dictionary words for passwords.
Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory to contain the "dictcheck" parameter:

```
dictcheck=1
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.330 RHEL-09-611110 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must enforce password complexity by requiring that at least one uppercase character be used.

```
GROUP ID: V-258111
RULE ID: SV-258111r1045226
```

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. Requiring a minimum number of uppercase characters makes password guessing attacks more difficult by ensuring a larger search space.

Audit:

Verify that RHEL 9 enforces password complexity by requiring that at least one uppercase character be used.
Check the value for "ucredit" with the following command:

```
$ grep ucredit /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf

ucredit = -1
```

If the value of "ucredit" is a positive number or is commented out, this is a finding.

Remediation:

Configure RHEL 9 to enforce password complexity by requiring that at least one uppercase character be used by setting the "ucredit" option.
Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory to contain the "ucredit" parameter:

```
ucredit = -1
```

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000192 The information system enforces password complexity by the minimum number of upper case characters used.

- NIST SP 800-53 :: IA-5 (1) (a)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (a)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.331 RHEL-09-611115 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must require the change of at least eight characters when passwords are changed.

```
GROUP ID: V-258112
RULE ID: SV-258112r1045229
```

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. Requiring a minimum number of different characters during password changes ensures that newly changed passwords will not resemble previously compromised ones. Note that passwords changed on compromised systems will still be compromised.

Audit:

Verify that RHEL 9 requires the change of at least eight of the total number of characters when passwords are changed.

```
$ grep difok /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf

difok = 8
```

If the value of "difok" is set to less than "8", or is commented out, this is a finding.

Remediation:

Configure RHEL 9 to require the change of at least eight of the total number of characters when passwords are changed by setting the "difok" option.
Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory to contain the "difok" parameter:

```
difok = 8
```

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000195 The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.

- NIST SP 800-53 :: IA-5 (1) (b)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (b)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.332 RHEL-09-611120 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must require the maximum number of repeating characters of the same character class be limited to four when passwords are changed.

```
GROUP ID: V-258113
RULE ID: SV-258113r1045232
```

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 a password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

Verify that RHEL 9 requires that passwords can have a maximum of four repeating characters of the same character class.

```
$ grep maxclassrepeat /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf

maxclassrepeat = 4
```

If the value of "maxclassrepeat" is set to "0", more than "4", or is commented out, this is a finding.

Remediation:

Configure RHEL 9 to require the change of the number of repeating characters of the same character class when passwords are changed by setting the "maxclassrepeat" option.
Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory to contain the "maxclassrepeat" parameter:

```
maxclassrepeat = 4
```

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000195 The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.

- NIST SP 800-53 :: IA-5 (1) (b)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (b)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.333 RHEL-09-611125 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must require the maximum number of repeating characters be limited to three when passwords are changed.

```
GROUP ID: V-258114
RULE ID: SV-258114r1045235
```

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 a password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

Verify that RHEL 9 requires that passwords can have a maximum of three of the same consecutive character.

```
$ grep maxrepeat /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf

maxrepeat = 3
```

If the value of "maxrepeat" is set to more than "3", or is commented out, this is a finding.

Remediation:

Configure RHEL 9 to require the change of the number of repeating consecutive characters when passwords are changed by setting the "maxrepeat" option.
Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory to contain the "maxrepeat" parameter:

```
maxrepeat = 3
```

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000195 The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.

- NIST SP 800-53 :: IA-5 (1) (b)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (b)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.334 RHEL-09-611130 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must require the change of at least four character classes when passwords are changed.

```
GROUP ID: V-258115
RULE ID: SV-258115r1045238
```

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 a password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

Verify that RHEL 9 requires passwords to contain at least four character classes.

```
$ grep minclass /etc/security/pwquality.conf
/etc/security/pwquality.conf.d/*.conf

minclass = 4
```

If the value of "minclass" is set to less than "4", or is commented out, this is a finding.

Remediation:

Configure RHEL 9 to require the change of at least four character classes when passwords are changed by setting the "minclass" option.
Add or update the following line in the "/etc/security/pwquality.conf" file or a configuration file in the "/etc/security/pwquality.conf.d/" directory to contain the "minclass" parameter:

```
minclass = 4
```

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (h)

CCI-000195 The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.

- NIST SP 800-53 :: IA-5 (1) (b)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (b)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.335 RHEL-09-611135 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must be configured so that user and group account administration utilities are configured to store only encrypted representations of passwords.

```
GROUP ID: V-258116
RULE ID: SV-258116r1045240
```

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 that are encrypted with a weak algorithm are no more protected than if they are kept in plain text.

This setting ensures user and group account administration utilities are configured to store only encrypted representations of passwords. Additionally, the "crypt_style" configuration option ensures the use of a strong hashing algorithm that makes password cracking attacks more difficult.

Audit:

Verify the user and group account administration utilities are configured to store only encrypted representations of passwords with the following command:

```
$ grep crypt_style /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 RHEL 9 to use the SHA-512 algorithm for password hashing.
Add or change the following line in the "[defaults]" section of "/etc/libuser.conf" file:

```
crypt_style = sha512
```

Additional Information:

CCI-004062 For password-based authentication, store passwords using an approved salted key derivation function, preferably using a keyed hash.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (d)

CCI-000196 The information system, for password-based authentication, stores only cryptographically-protected passwords.

- NIST SP 800-53 :: IA-5 (1) (c)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (c)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.336 RHEL-09-611140 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must be configured to use the shadow file to store only encrypted representations of passwords.

```
GROUP ID: V-258117
RULE ID: SV-258117r1015116
```

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 that are encrypted with a weak algorithm are no more protected than if they are kept in plain text.

This setting ensures user and group account administration utilities are configured to store only encrypted representations of passwords. Additionally, the "crypt_style" configuration option ensures the use of a strong hashing algorithm that makes password cracking attacks more difficult.

Audit:

Verify the system's shadow file is configured to store only encrypted representations of passwords with a hash value of SHA512 with the following command:

```
# grep -i encrypt_method /etc/login.defs

ENCRYPT_METHOD SHA512
```

If "ENCRYPT_METHOD" does not have a value of "SHA512", or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to store only SHA512 encrypted representations of passwords.
Add or update the following line in the "/etc/login.defs" file:

```
ENCRYPT_METHOD SHA512
```

Additional Information:

CCI-004062 For password-based authentication, store passwords using an approved salted key derivation function, preferably using a keyed hash.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (d)

CCI-000196 The information system, for password-based authentication, stores only cryptographically-protected passwords.

- NIST SP 800-53 :: IA-5 (1) (c)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (c)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.337 RHEL-09-611145 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not be configured to bypass password requirements for privilege escalation.

```
GROUP ID: V-258118
RULE ID: SV-258118r1050789
```

Rationale:

Without reauthentication, 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 reauthenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Audit:

Verify the operating system is not configured to bypass password requirements for privilege escalation with the following command:

```
$ sudo grep pam_succeed_if /etc/pam.d/sudo
```

If any occurrences of "pam_succeed_if" are returned, this is a finding.

Remediation:

Configure the operating system to require users to supply a password for privilege escalation.
Remove any occurrences of " pam_succeed_if " in the "/etc/pam.d/sudo" file.

Additional Information:

CCI-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5 :: SC-11 b

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4 :: IA-11

1.338 RHEL-09-611155 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must not have accounts configured with blank or null passwords.

```
GROUP ID: V-258120
RULE ID: SV-258120r991589
```

Rationale:

If an account has an empty password, anyone could log in and run commands with the privileges of that account. Accounts with empty passwords should never be used in operational environments.

Audit:

Verify that null or blank passwords cannot be used with the following command:

```
$ sudo awk -F: '!$2 {print $1}' /etc/shadow
```

If the command returns any results, this is a finding.

Remediation:

Configure all accounts on RHEL 9 to have a password or lock the account with the following commands:
Perform a password reset:

```
$ sudo passwd [username]
```

To lock an account:

```
$ sudo passwd -l [username]
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.339 RHEL-09-611160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must use the common access card (CAC) smart card driver.

```
GROUP ID: V-258121
RULE ID: SV-258121r1045243
```

Rationale:

Smart card login provides two-factor authentication stronger than that provided by a username and password combination. Smart cards leverage public key infrastructure to provide and verify credentials. Configuring the smart card driver in use by the organization helps to prevent users from using unauthorized smart cards.

Satisfies: SRG-OS-000104-GPOS-00051, SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000109-GPOS-00056, SRG-OS-000108-GPOS-00055, SRG-OS-000112-GPOS-00057, SRG-OS-000113-GPOS-00058

Audit:

Verify that RHEL loads the CAC driver with the following command:

```
$ sudo opensc-tool --get-conf-entry app:default:card_driver cac

cac
```

If "cac" is not listed as a card driver, or no line is returned for "card_drivers", this is a finding.

Remediation:

Configure RHEL 9 to load the CAC driver.

```
$ sudo opensc-tool --set-conf-entry app:default:card_driver:cac
```

Restart the pcscd service to apply the changes:

```
$ sudo systemctl restart pcscd
```

Additional Information:

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53 :: IA-2
- NIST SP 800-53 Revision 4 :: IA-2
- NIST SP 800-53 Revision 5 :: IA-2
- NIST SP 800-53A :: IA-2.1

CCI-000766 Implement multifactor authentication for network access to non-privileged accounts.

- NIST SP 800-53 :: IA-2 (2)
- NIST SP 800-53 Revision 4 :: IA-2 (2)
- NIST SP 800-53 Revision 5 :: IA-2 (2)
- NIST SP 800-53A :: IA-2 (2).1

CCI-000765 Implement multifactor authentication for network access to privileged accounts.

- NIST SP 800-53 :: IA-2 (1)
- NIST SP 800-53 Revision 4 :: IA-2 (1)
- NIST SP 800-53 Revision 5 :: IA-2 (1)
- NIST SP 800-53A :: IA-2 (1).1

CCI-004045 Require users to be individually authenticated before granting access to the shared accounts or resources.

- NIST SP 800-53 Revision 5 :: IA-2 (5)

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4 :: IA-2 (8)
- NIST SP 800-53 Revision 5 :: IA-2 (8)

CCI-000767 The information system implements multifactor authentication for local access to privileged accounts.

- NIST SP 800-53 :: IA-2 (3)
- NIST SP 800-53 Revision 4 :: IA-2 (3)
- NIST SP 800-53A :: IA-2 (3).1

CCI-000768 The information system implements multifactor authentication for local access to non-privileged accounts.

- NIST SP 800-53 :: IA-2 (4)
- NIST SP 800-53 Revision 4 :: IA-2 (4)
- NIST SP 800-53A :: IA-2 (4).1

CCI-000770 The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

- NIST SP 800-53 :: IA-2 (5) (b)
- NIST SP 800-53 Revision 4 :: IA-2 (5)
- NIST SP 800-53A :: IA-2 (5).2 (ii)

CCI-001942 The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

- NIST SP 800-53 Revision 4 :: IA-2 (9)

1.340 RHEL-09-611165 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must enable certificate based smart card authentication.

```
GROUP ID: V-258122
RULE ID: SV-258122r1045246
```

Rationale:

Without the use of multifactor authentication, the ease of access to privileged functions is greatly increased. Multifactor authentication requires using two or more factors to achieve authentication. A privileged account is defined as an information system account with authorizations of a privileged user. The DOD Common Access Card (CAC) with DOD-approved PKI is an example of multifactor authentication.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000105-GPOS-00052

Audit:

Note: If the system administrator (SA) demonstrates the use of an approved alternate multifactor authentication method, this requirement is Not Applicable.
To verify that RHEL 9 has smart cards enabled in System Security Services Daemon (SSSD), run the following command:

```
$ sudo grep -ir pam_cert_auth /etc/sssd/sssd.conf /etc/sssd/conf.d/

pam_cert_auth = True
```

If "pam_cert_auth" is not set to "True", the line is commented out, or the line is missing, this is a finding.

Remediation:

Edit the file "/etc/sssd/sssd.conf" or a configuration file in "/etc/sssd/conf.d" and add or edit the following line:

```
pam_cert_auth = True
```

Additional Information:

CCI-000765 Implement multifactor authentication for network access to privileged accounts.

- NIST SP 800-53 :: IA-2 (1)
- NIST SP 800-53 Revision 4 :: IA-2 (1)
- NIST SP 800-53 Revision 5 :: IA-2 (1)
- NIST SP 800-53A :: IA-2 (1).1

CCI-004046 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 5 :: IA-2 (6) (a)

CCI-004047 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that the device meets organization-defined strength of mechanism requirements.

- NIST SP 800-53 Revision 5 :: IA-2 (6) (b)

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.

- NIST SP 800-53 Revision 4 :: IA-2 (11)

1.341 RHEL-09-611170 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must implement certificate status checking for multifactor authentication.

```
GROUP ID: V-258123
RULE ID: SV-258123r1045248
```

Rationale:

Using an authentication device, such as a DOD common access card (CAC) or token that is separate from the information system, ensures that even if the information system is compromised, credentials stored on the authentication device will not be affected.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification (PIV) card and the DOD CAC.

RHEL 9 includes multiple options for configuring certificate status checking, but for this requirement focuses on the System Security Services Daemon (SSSD). By default, SSSD performs Online Certificate Status Protocol (OCSP) checking and certificate verification using a sha256 digest function.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000377-GPOS-00162

Audit:

Note: If the system administrator (SA) demonstrates the use of an approved alternate multifactor authentication method, this requirement is Not Applicable.
Verify the operating system implements Online Certificate Status Protocol (OCSP) and is using the proper digest value on the system with the following command:

```
$ sudo grep -ir certificate_verification /etc/sssd/sssd.conf
/etc/sssd/conf.d/ | grep -v "^#"

certificate_verification = ocsp_dgst=sha512
```

If the certificate_verification line is missing from the [sssd] section, or is missing "ocsp_dgst=sha512", ask the administrator to indicate what type of multifactor authentication is being used and how the system implements certificate status checking. If there is no evidence of certificate status checking being used, this is a finding.

Remediation:

Configure RHEL 9 to implement certificate status checking for multifactor authentication. Review the "/etc/sssd/conf.d/certificate_verification.conf" file to determine if the system is configured to prevent OCSP or certificate verification.
Add the following line to the "/etc/sssd/conf.d/certificate_verification.conf" file:

```
certificate_verification = ocsp_dgst=sha512
```

Set the correct ownership and permissions on the "/etc/sssd/conf.d/certificate_verification.conf" file by running these commands:

```
$ sudo chown root:root "/etc/sssd/conf.d/certificate_verification.conf"
$ sudo chmod 600 "/etc/sssd/conf.d/certificate_verification.conf"
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
$ sudo systemctl restart sssd.service
```

Additional Information:

CCI-004046 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 5 :: IA-2 (6) (a)

CCI-001954 Electronically verifies Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4 :: IA-2 (12)
- NIST SP 800-53 Revision 5 :: IA-2 (12)

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.

- NIST SP 800-53 Revision 4 :: IA-2 (11)

1.342 RHEL-09-611175 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must have the pcsc-lite package installed.

```
GROUP ID: V-258124
RULE ID: SV-258124r1045250
```

Rationale:

The pcsc-lite package must be installed if it is to be available for multifactor authentication using smart cards.

Audit:

Note: If the system administrator (SA) demonstrates the use of an approved alternate multifactor authentication method, this requirement is Not Applicable.
Verify that RHEL 9 has the pcsc-lite package installed with the following command:

```
$ dnf list --installed pcsc-lite
```

Example output:

```
pcsc-lite.x86_64          1.9.4-1.el9
```

If the "pcsc-lite" package is not installed, this is a finding.

Remediation:

The pcsc-lite package can be installed with the following command:

```
$ sudo dnf install pcsc-lite
```

Additional Information:

CCI-004046 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 5 :: IA-2 (6) (a)

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.

- NIST SP 800-53 Revision 4 :: IA-2 (11)

1.343 RHEL-09-611180 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The pcscd service on RHEL 9 must be active.

```
GROUP ID: V-258125
RULE ID: SV-258125r1045253
```

Rationale:

The information system ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

The daemon program for pcsc-lite and the MuscleCard framework is pcscd. It is a resource manager that coordinates communications with smart card readers and smart cards and cryptographic tokens that are connected to the system.

Audit:

Verify that the "pcscd" socket is active with the following command:

```
$ systemctl is-active pcscd.socket

active
```

If the pcscd socket is not active, this is a finding.

Remediation:

To enable the pcscd socket, run the following command:

```
$ sudo systemctl enable --now pcscd.socket
```

Additional Information:

CCI-004046 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 5 :: IA-2 (6) (a)

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.

- NIST SP 800-53 Revision 4 :: IA-2 (11)

1.344 RHEL-09-611185 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must have the opensc package installed.

```
GROUP ID: V-258126
RULE ID: SV-258126r1045255
```

Rationale:

The use of PIV credentials facilitates standardization and reduces the risk of unauthorized access.

The DOD has mandated the use of the common access card (CAC) to support identity management and personal authentication for systems covered under Homeland Security Presidential Directive (HSPD) 12, as well as making the CAC a primary component of layered protection for national security systems.

Satisfies: SRG-OS-000375-GPOS-00160, SRG-OS-000376-GPOS-00161

Audit:

Verify that RHEL 9 has the opensc package installed with the following command:

```
$ dnf list --installed opensc
```

Example output:

```
opensc.x86_64          0.22.0-2.el9
```

If the "opensc" package is not installed, this is a finding.

Remediation:

The opensc package can be installed with the following command:

```
$ sudo dnf install opensc
```

Additional Information:

CCI-004046 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 5 :: IA-2 (6) (a)

CCI-001953 Accepts Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4 :: IA-2 (12)
- NIST SP 800-53 Revision 5 :: IA-2 (12)

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.

- NIST SP 800-53 Revision 4 :: IA-2 (11)

1.345 RHEL-09-611190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9, for PKI-based authentication, must enforce authorized access to the corresponding private key.

```
GROUP ID: V-258127
RULE ID: SV-258127r958450
```

Rationale:

If the private key is discovered, an attacker can use the key to authenticate as an authorized user and gain access to the network infrastructure.

The cornerstone of the PKI is the private key used to encrypt or digitally sign information.

If the private key is stolen, this will lead to the compromise of the authentication and nonrepudiation gained through PKI because the attacker can use the private key to digitally sign documents and pretend to be the authorized user.

Both the holders of a digital certificate and the issuing authority must protect the computers, storage devices, or whatever they use to keep the private keys.

Audit:

Verify the SSH private key files have a passcode.
For each private key stored on the system, use the following command:

```
$ sudo ssh-keygen -y -f /path/to/file
```

If the contents of the key are displayed, this is a finding.

Remediation:

Create a new private and public key pair that utilizes a passcode with the following command:

```
$ sudo ssh-keygen -n [passphrase]
```

Additional Information:

CCI-000186 For public key-based authentication, enforce authorized access to the corresponding private key.

- NIST SP 800-53 :: IA-5 (2)
- NIST SP 800-53 Revision 4 :: IA-5 (2) (b)
- NIST SP 800-53 Revision 5 :: IA-5 (2) (a) (1)
- NIST SP 800-53A :: IA-5 (2).1

1.346 RHEL-09-611195 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must require authentication to access emergency mode.

```
GROUP ID: V-258128
RULE ID: SV-258128r958472
```

Rationale:

To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DOD-approved PKIs, all DOD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

This requirement prevents attackers with physical access from trivially bypassing security on the machine and gaining root access. Such accesses are further prevented by configuring the bootloader password.

Audit:

Verify that RHEL 9 requires authentication for emergency mode with the following command:

```
$ grep sulogin /usr/lib/systemd/system/emergency.service

ExecStart=-/usr/lib/systemd/systemd-sulogin-shell emergency
```

If this line is not returned, or is commented out, this is a finding. If the output is different, this is a finding.

Remediation:

Configure RHEL 9 to require authentication for emergency mode.
Add or modify the following line in the "/usr/lib/systemd/system/emergency.service" file:

```
ExecStart=-/usr/lib/systemd/systemd-sulogin-shell emergency
```

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53 :: AC-3
- NIST SP 800-53 Revision 4 :: AC-3
- NIST SP 800-53 Revision 5 :: AC-3
- NIST SP 800-53A :: AC-3.1

1.347 RHEL-09-611200 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must require authentication to access single-user mode.

```
GROUP ID: V-258129
RULE ID: SV-258129r958472
```

Rationale:

To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DOD-approved PKIs, all DOD systems (e.g., web servers and web portals) must be properly configured to incorporate access control methods that do not rely solely on the possession of a certificate for access. Successful authentication must not automatically give an entity access to an asset or security boundary. Authorization procedures and controls must be implemented to ensure each authenticated entity also has a validated and current authorization. Authorization is the process of determining whether an entity, once authenticated, is permitted to access a specific asset. Information systems use access control policies and enforcement mechanisms to implement this requirement.

This requirement prevents attackers with physical access from trivially bypassing security on the machine and gaining root access. Such accesses are further prevented by configuring the bootloader password.

Audit:

Verify that RHEL 9 requires authentication for single-user mode with the following command:

```
$ grep sulogin /usr/lib/systemd/system/rescue.service

ExecStart=-/usr/lib/systemd/systemd-sulogin-shell rescue
```

If this line is not returned, or is commented out, this is a finding.

Remediation:

Configure RHEL 9 to require authentication for single-user mode.
Add or modify the following line in the "/usr/lib/systemd/system/rescue.service" file:

```
ExecStart=-/usr/lib/systemd/systemd-sulogin-shell rescue
```

Additional Information:

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53 :: AC-3
- NIST SP 800-53 Revision 4 :: AC-3
- NIST SP 800-53 Revision 5 :: AC-3
- NIST SP 800-53A :: AC-3.1

1.348 RHEL-09-631010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9, for PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.

```
GROUP ID: V-258131
RULE ID: SV-258131r1015125
```

Rationale:

Without path validation, an informed trust decision by the relying party cannot be made when presented with any certificate not already explicitly trusted.

A trust anchor is an authoritative entity represented via a public key and associated data. It is used in the context of public key infrastructures, X.509 digital certificates, and DNSSEC.

When there is a chain of trust, usually the top entity to be trusted becomes the trust anchor; it can be, for example, a certification authority (CA). A certification path starts with the subject certificate and proceeds through a number of intermediate certificates up to a trusted root certificate, typically issued by a trusted CA.

This requirement verifies that a certification path to an accepted trust anchor is used for certificate validation and that the path includes status information. Path validation is necessary for a relying party to make an informed trust decision when presented with any certificate not already explicitly trusted. Status information for certification paths includes certificate revocation lists or online certificate status protocol responses. Validation of the certificate status information is out of scope for this requirement.

Satisfies: SRG-OS-000066-GPOS-00034, SRG-OS-000384-GPOS-00167

Audit:

Verify RHEL 9 for PKI-based authentication has valid certificates by constructing a certification path (which includes status information) to an accepted trust anchor. Check that the system has a valid DOD root CA installed with the following command:

```
$ sudo openssl x509 -text -in /etc/sssd/pki/sssd_auth_ca_db.pem
```

Example output:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = U.S. Government, OU = DoD, OU = PKI, CN = DoD
Root CA 3
        Validity
        Not Before: Mar 20 18:46:41 2012 GMT
        Not After: Dec 30 18:46:41 2029 GMT
        Subject: C = US, O = U.S. Government, OU = DoD, OU = PKI, CN = DoD
Root CA 3
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
```

If the root CA file is not a DOD-issued certificate with a valid date and installed in the "/etc/sssd/pki/sssd_auth_ca_db.pem" location, this is a finding.

Remediation:

Configure RHEL 9, for PKI-based authentication, to validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor. Obtain a valid copy of the DOD root CA file from the PKI CA certificate bundle from cyber.mil and copy the DoD_PKE_CA_chain.pem into the following file:

```
/etc/sssd/pki/sssd_auth_ca_db.pem
```

Additional Information:

CCI-000185 For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

- NIST SP 800-53 :: IA-5 (2)
- NIST SP 800-53 Revision 4 :: IA-5 (2) (a)
- NIST SP 800-53 Revision 5 :: IA-5 (2) (b) (1)
- NIST SP 800-53A :: IA-5 (2).1

CCI-004068 For public key-based authentication, implement a local cache of revocation data to support path discovery and validation.

- NIST SP 800-53 Revision 5 :: IA-5 (2) (b) (2)

CCI-001991 The information system, for PKI-based authentication, implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

- NIST SP 800-53 Revision 4 :: IA-5 (2) (d)

1.349 RHEL-09-631015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must map the authenticated identity to the user or group account for PKI-based authentication.

```
GROUP ID: V-258132
RULE ID: SV-258132r1045260
```

Rationale:

Without mapping the certificate used to authenticate to the user account, the ability to determine the identity of the individual user or group will not be available for forensic analysis.

Audit:

Verify the certificate of the user or group is mapped to the corresponding user or group in the "sssd.conf" file with the following command:

```
$ sudo find /etc/sssd/sssd.conf /etc/sssd/conf.d/ -type f -exec cat {} \;

[certmap/testing.test/rule_name]
matchrule =<SAN>.*EDIPI@mil
maprule = (userCertificate;binary={cert!bin})
domains = testing.test
```

If the certmap section does not exist, ask the system administrator (SA) to indicate how certificates are mapped to accounts.
If there is no evidence of certificate mapping, this is a finding.

Remediation:

Configure RHEL 9 to map the authenticated identity to the user or group account by adding or modifying the certmap section of the "/etc/sssd/sssd.conf" file based on the following example:

```
[certmap/testing.test/rule_name]
matchrule = .*EDIPI@mil
maprule = (userCertificate;binary={cert!bin})
domains = testing.test
```

The "sssd" service must be restarted for the changes to take effect. To restart the "sssd" service, run the following command:

```
$ sudo systemctl restart sssd.service
```

Additional Information:

CCI-000187 For public key-based authentication, map the authenticated identity to the account of the individual or group.

- NIST SP 800-53 :: IA-5 (2)
- NIST SP 800-53 Revision 4 :: IA-5 (2) (c)
- NIST SP 800-53 Revision 5 :: IA-5 (2) (a) (2)
- NIST SP 800-53A :: IA-5 (2).1

1.350 RHEL-09-631020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must prohibit the use of cached authenticators after one day.

```
GROUP ID: V-258133
RULE ID: SV-258133r1045263
```

Rationale:

If cached authentication information is out-of-date, the validity of the authentication information may be questionable.

Audit:

Verify that the System Security Services Daemon (SSSD) prohibits the use of cached authentications after one day.
Note: Cached authentication settings should be configured even if smart card authentication is not used on the system.
Check that SSSD allows cached authentications with the following command:

```
$ sudo grep -ir cache_credentials /etc/sssd/sssd.conf /etc/sssd/conf.d/

cache_credentials = true
```

If "cache_credentials" is set to "false" or missing from the configuration file, this is not a finding and no further checks are required.
If "cache_credentials" is set to "true", check that SSSD prohibits the use of cached authentications after one day with the following command:

```
$ sudo grep -ir offline_credentials_expiration /etc/sssd/sssd.conf
/etc/sssd/conf.d/

offline_credentials_expiration = 1
```

If "offline_credentials_expiration" is not set to a value of "1", this is a finding.

Remediation:

Configure the SSSD to prohibit the use of cached authentications after one day.
Edit the file "/etc/sssd/sssd.conf" or a configuration file in "/etc/sssd/conf.d" and add or edit the following line just below the line [pam]:

```
offline_credentials_expiration = 1
```

Additional Information:

CCI-002007 Prohibit the use of cached authenticators after an organization-defined time period.

- NIST SP 800-53 Revision 4 :: IA-5 (13)
- NIST SP 800-53 Revision 5 :: IA-5 (13)

1.351 RHEL-09-651010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must have the AIDE package installed.

```
GROUP ID: V-258134
RULE ID: SV-258134r1045265
```

Rationale:

Without verification of the security functions, security functions may not operate correctly, and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

Satisfies: SRG-OS-000363-GPOS-00150, SRG-OS-000445-GPOS-00199

Audit:

Verify that RHEL 9 has the Advanced Intrusion Detection Environment (AIDE) package installed with the following command:

```
$ dnf list --installed aide
```

Example output:

```
aide.x86_64          0.16.100.el9
```

If AIDE is not installed, ask the system administrator (SA) how file integrity checks are performed on the system.
If there is no application installed to perform integrity checks, this is a finding.
If AIDE is installed, check if it has been initialized with the following command:

```
$ sudo /usr/sbin/aide --check
```

If the output is "Couldn't open file /var/lib/aide/aide.db.gz for reading", this is a finding.

Remediation:

Install AIDE, initialize it, and perform a manual check.
Install AIDE:

```
$ sudo dnf install aide
```

Initialize AIDE:

```
$ sudo /usr/sbin/aide --init
```

Example output:

```
Start timestamp: 2023-06-05 10:09:04 -0600 (AIDE 0.16)
AIDE initialized database at /var/lib/aide/aide.db.new.gz

Number of entries:      86833

---------------------------------------------------
The attributes of the (uncompressed) database(s):
---------------------------------------------------

/var/lib/aide/aide.db.new.gz
  MD5      : coZUtPHhoFoeD7+k54fUvQ==
  SHA1     : DVpOEMWJwo0uPgrKZAygIUgSxeM=
  SHA256   : EQiZH0XNEk001tcDmJa+5STFEjDb4MPE
             TGdBJ/uvZKc=
  SHA512   : 86KUqw++PZhoPK0SZvT3zuFq9yu9nnPP
             toei0nENVELJ1LPurjoMlRig6q69VR8l
             +44EwO9eYyy9nnbzQsfG1g==

End timestamp: 2023-06-05 10:09:57 -0600 (run time: 0m 53s)
```

The new database will need to be renamed to be read by AIDE:

```
$ sudo mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

Perform a manual check:

```
$ sudo /usr/sbin/aide --check
```

Example output:

```
2023-06-05 10:16:08 -0600 (AIDE 0.16)
AIDE found NO differences between database and filesystem. Looks okay!!

...
```

Additional Information:

CCI-001744 Implement organization-defined security responses automatically if baseline configurations are changed in an unauthorized manner.

- NIST SP 800-53 Revision 4 :: CM-3 (5)
- NIST SP 800-53 Revision 5 :: CM-3 (5)

CCI-002696 Verify correct operation of organization-defined security functions.

- NIST SP 800-53 Revision 4 :: SI-6 a
- NIST SP 800-53 Revision 5 :: SI-6 a

1.352 RHEL-09-651015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must routinely check the baseline configuration for unauthorized changes and notify the system administrator when anomalies in the operation of any security functions are discovered.

```
GROUP ID: V-258135
RULE ID: SV-258135r1045267
```

Rationale:

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating system's information management officer (IMO)/information system security officer (ISSO) and system administrators (SAs) must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

Notifications provided by information systems include messages to local computer consoles, and/or hardware indications, such as lights.

This capability must take into account operational requirements for availability for selecting an appropriate response. The organization may choose to shut down or restart the information system upon security function anomaly detection.

Satisfies: SRG-OS-000363-GPOS-00150, SRG-OS-000446-GPOS-00200, SRG-OS-000447-GPOS-00201

Audit:

Verify that RHEL 9 routinely executes a file integrity scan for changes to the system baseline. The command used in the example will use a daily occurrence.
Check the cron directories for scripts controlling the execution and notification of results of the file integrity application. For example, if AIDE is installed on the system, use the following commands:

```
$ sudo ls -al /etc/cron.* | grep aide

-rwxr-xr-x 1 root root 29 Nov 22 2015 aide

$ sudo grep aide /etc/crontab /var/spool/cron/root

/etc/crontab: 30 04 * * * root usr/sbin/aide
/var/spool/cron/root: 30 04 * * * root usr/sbin/aide

$ sudo more /etc/cron.daily/aide

#!/bin/bash
/usr/sbin/aide --check | /bin/mail -s "$HOSTNAME - Daily aide integrity check
run" root@sysname.mil
```

If the file integrity application does not exist, a script file controlling the execution of the file integrity application does not exist, or the file integrity application does not notify designated personnel of changes, this is a finding.

Remediation:

Configure the file integrity tool to run automatically on the system at least weekly and to notify designated personnel if baseline configurations are changed in an unauthorized manner. The AIDE tool can be configured to email designated personnel with the use of the cron system.
The following example output is generic. It will set cron to run AIDE daily and to send email at the completion of the analysis

```
$ sudo more /etc/cron.daily/aide

#!/bin/bash
/usr/sbin/aide --check | /bin/mail -s "$HOSTNAME - Daily aide integrity check
run" root@sysname.mil
```

Additional Information:

CCI-001744 Implement organization-defined security responses automatically if baseline configurations are changed in an unauthorized manner.

- NIST SP 800-53 Revision 4 :: CM-3 (5)
- NIST SP 800-53 Revision 5 :: CM-3 (5)

CCI-002699 Perform verification of the correct operation of organization-defined security functions: when the system is in an organization-defined transitional state; upon command by a user with appropriate privileges; and/or on an organization-defined frequency.

- NIST SP 800-53 Revision 4 :: SI-6 b
- NIST SP 800-53 Revision 5 :: SI-6 b

CCI-002702 Shut the system down, restart the system, and/or initiate organization-defined alternative action(s) when anomalies in the operation of the organization-defined security functions are discovered.

- NIST SP 800-53 Revision 4 :: SI-6 d
- NIST SP 800-53 Revision 5 :: SI-6 d

1.353 RHEL-09-651020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must use a file integrity tool that is configured to use FIPS 140-3-approved cryptographic hashes for validating file contents and directories.

```
GROUP ID: V-258136
RULE ID: SV-258136r1045270
```

Rationale:

RHEL 9 installation media ships with an optional file integrity tool called Advanced Intrusion Detection Environment (AIDE). AIDE is highly configurable at install time. This requirement assumes the "aide.conf" file is under the "/etc" directory.

File integrity tools use cryptographic hashes for verifying file contents and directories have not been altered. These hashes must be FIPS 140-3-approved cryptographic hashes.

Audit:

Verify that AIDE is configured to use FIPS 140-3 file hashing with the following command:

```
$ sudo grep sha512 /etc/aide.conf

All=p+i+n+u+g+s+m+S+sha512+acl+xattrs+selinux
```

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 140-3-approved cryptographic hashes for validating file contents and directories, this is a finding.

Remediation:

Configure the file integrity tool to use FIPS 140-3 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. Exclude any log files, or files expected to change frequently, to reduce unnecessary notifications.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.354 RHEL-09-651025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must use cryptographic mechanisms to protect the integrity of audit tools.

```
GROUP ID: V-258137
RULE ID: SV-258137r1045272
```

Rationale:

Protecting the integrity of the tools used for auditing purposes is a critical step toward ensuring the integrity of audit information. Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Audit tools include, but are not limited to, vendor-provided and open-source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

It is not uncommon for attackers to replace the audit tools or inject code into the existing tools to provide the capability to hide or erase system activity from the audit logs.

To address this risk, audit tools must be cryptographically signed to provide the capability to identify when the audit tools have been modified, manipulated, or replaced. An example is a checksum hash of the file or files.

Satisfies: SRG-OS-000256-GPOS-00097, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099, SRG-OS-000278-GPOS-00108

Audit:

Check that AIDE is properly configured to protect the integrity of the audit tools with the following command:

```
$ sudo grep /usr/bin/au /etc/aide.conf

/usr/sbin/auditctl p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/auditd p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/ausearch p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/aureport p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/autrace p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/augenrules p+i+n+u+g+s+b+acl+xattrs+sha512
```

If AIDE is not installed, ask the system administrator (SA) how file integrity checks are performed on the system.
If any of the audit tools listed above do not have a corresponding line, ask the SA to indicate what cryptographic mechanisms are being used to protect the integrity of the audit tools.
If there is no evidence of integrity protection, this is a finding.

Remediation:

Add or update the following lines to "/etc/aide.conf", to protect the integrity of the audit tools.

```
/usr/sbin/auditctl p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/auditd p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/ausearch p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/aureport p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/autrace p+i+n+u+g+s+b+acl+xattrs+sha512
/usr/sbin/augenrules p+i+n+u+g+s+b+acl+xattrs+sha512
```

Additional Information:

CCI-001493 Protect audit tools from unauthorized access.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9
- NIST SP 800-53A :: AU-9.1

CCI-001495 Protect audit tools from unauthorized deletion.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9
- NIST SP 800-53A :: AU-9.1

CCI-001496 Implement cryptographic mechanisms to protect the integrity of audit tools.

- NIST SP 800-53 :: AU-9 (3)
- NIST SP 800-53 Revision 4 :: AU-9 (3)
- NIST SP 800-53 Revision 5 :: AU-9 (3)
- NIST SP 800-53A :: AU-9 (3).1

1.355 RHEL-09-651030 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

RHEL 9 must be configured so that the file integrity tool verifies Access Control Lists (ACLs).

```
GROUP ID: V-258138
RULE ID: SV-258138r1045274
```

Rationale:

RHEL 9 installation media ships with an optional file integrity tool called Advanced Intrusion Detection Environment (AIDE). AIDE is highly configurable at install time. This requirement assumes the "aide.conf" file is under the "/etc" directory.

ACLs can provide permissions beyond those permitted through the file mode and must be verified by the file integrity tools.

Audit:

Verify that AIDE is verifying ACLs with the following command:

```
$ sudo grep acl /etc/aide.conf

All= p+i+n+u+g+s+m+S+sha512+acl+xattrs+selinux
```

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, this is a finding.

Remediation:

Configure the file integrity tool to check file and directory ACLs.
If AIDE is installed, ensure the "acl" rule is present on all uncommented file and directory selection lists.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.356 RHEL-09-651035 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

RHEL 9 must be configured so that the file integrity tool verifies extended attributes.

```
GROUP ID: V-258139
RULE ID: SV-258139r1045276
```

Rationale:

RHEL 9 installation media ships with an optional file integrity tool called Advanced Intrusion Detection Environment (AIDE). AIDE is highly configurable at install time. This requirement assumes the "aide.conf" file is under the "/etc" directory.

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

Audit:

Verify that AIDE is configured to verify extended attributes with the following command:

```
$ sudo grep xattrs /etc/aide.conf

All= p+i+n+u+g+s+m+S+sha512+acl+xattrs+selinux
```

If the "xattrs" rule is not being used on all uncommented selection lines in the "/etc/aide.conf" file, or extended attributes are not being checked by another file integrity tool, this is a finding.

Remediation:

Configure the file integrity tool to check file and directory extended attributes.
If AIDE is installed, ensure the "xattrs" rule is present on all uncommented file and directory selection lists.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.357 RHEL-09-652010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must have the rsyslog package installed.

```
GROUP ID: V-258140
RULE ID: SV-258140r1045278
```

Rationale:

rsyslogd is a system utility providing support for message logging. Support for both internet and Unix domain sockets enables this utility to support both local and remote logging. Couple this utility with "gnutls" (which is a secure communications library implementing the SSL, TLS, and DTLS protocols), to create a method to securely encrypt and offload auditing.

Satisfies: SRG-OS-000479-GPOS-00224, SRG-OS-000051-GPOS-00024, SRG-OS-000480-GPOS-00227

Audit:

Verify that RHEL 9 has the rsyslogd package installed with the following command:

```
$ dnf list --installed rsyslog
```

Example output:

```
rsyslog.x86_64          8.2102.0-101.el9_0.1
```

If the "rsyslogd" package is not installed, this is a finding.

Remediation:

The rsyslogd package can be installed with the following command:

```
$ sudo dnf install rsyslogd
```

Additional Information:

CCI-000154 Provide the capability to centrally review and analyze audit records from multiple components within the system.

- NIST SP 800-53 :: AU-6 (4)
- NIST SP 800-53 Revision 4 :: AU-6 (4)
- NIST SP 800-53 Revision 5 :: AU-6 (4)
- NIST SP 800-53A :: AU-6 (4).1

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4 :: AU-4 (1)
- NIST SP 800-53 Revision 5 :: AU-4 (1)

1.358 RHEL-09-652015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must have the packages required for encrypting offloaded audit logs installed.

```
GROUP ID: V-258141
RULE ID: SV-258141r1045280
```

Rationale:

The rsyslog-gnutls package provides Transport Layer Security (TLS) support for the rsyslog daemon, which enables secure remote logging.

Satisfies: SRG-OS-000480-GPOS-00227, SRG-OS-000120-GPOS-00061

Audit:

Verify that RHEL 9 has the rsyslog-gnutls package installed with the following command:

```
$ dnf list --installed rsyslog-gnutls
```

Example output:

```
rsyslog-gnutls.x86_64          8.2102.0-101.el9_0.1
```

If the "rsyslog-gnutls" package is not installed, this is a finding.

Remediation:

The rsyslog-gnutls package can be installed with the following command:

```
$ sudo dnf install rsyslog-gnutls
```

Additional Information:

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53 :: IA-7
- NIST SP 800-53 Revision 4 :: IA-7
- NIST SP 800-53 Revision 5 :: IA-7
- NIST SP 800-53A :: IA-7.1

1.359 RHEL-09-652020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

The rsyslog service on RHEL 9 must be active.

```
GROUP ID: V-258142
RULE ID: SV-258142r991589
```

Rationale:

The "rsyslog" service must be running to provide logging services, which are essential to system administration.

Audit:

Verify that "rsyslog" is active with the following command:

```
$ systemctl is-active rsyslog

active
```

If the rsyslog service is not active, this is a finding.

Remediation:

To enable the rsyslog service, run the following command:

```
$ sudo systemctl enable --now rsyslog
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.360 RHEL-09-652025 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must be configured so that the rsyslog daemon does not accept log messages from other servers unless the server is being used for log aggregation.

```
GROUP ID: V-258143
RULE ID: SV-258143r1045283
```

Rationale:

Unintentionally running a rsyslog server accepting remote messages puts the system at increased risk. Malicious rsyslog messages sent to the server could exploit vulnerabilities in the server software itself, could introduce misleading information into the system's logs, or could fill the system's storage leading to a denial of service.

If the system is intended to be a log aggregation server, its use must be documented with the information system security officer (ISSO).

Audit:

Verify that RHEL 9 is not configured to receive remote logs using rsyslog with the following commands:

```
$ grep -i modload /etc/rsyslog.conf /etc/rsyslog.d/*

$ModLoad imtcp
$ModLoad imrelp
$ModLoad imudp

$ grep -i 'load="imtcp"' /etc/rsyslog.conf /etc/rsyslog.d/*

$ grep -i 'load="imrelp"' /etc/rsyslog.conf /etc/rsyslog.d/*

$ grep -i serverrun /etc/rsyslog.conf /etc/rsyslog.d/*

$InputTCPServerRun 514
$InputRELPServerRun 514
$InputUDPServerRun 514

$ grep -i 'port="\S*"' /etc/rsyslog.conf /etc/rsyslog.d/*

/etc/rsyslog.conf:#input(type="imudp" port="514")
/etc/rsyslog.conf:#input(type="imtcp" port="514")
/etc/rsyslog.conf:#Target="remote_host" Port="XXX" Protocol="tcp")
```

If any uncommented lines are returned by the commands, rsyslog is configured to receive remote messages, and this is a finding.
Note: An error about no files or directories from the above commands may be returned. This is not a finding.
If any modules are being loaded in the "/etc/rsyslog.conf" file or in the "/etc/rsyslog.d" subdirectories, ask to see the documentation for the system being used for log aggregation.
If the documentation does not exist or does not specify the server as a log aggregation system, this is a finding.

Remediation:

Configure RHEL 9 to not receive remote logs using rsyslog.
Remove the lines in /etc/rsyslog.conf and any files in the /etc/rsyslog.d directory that match any of the following:

```
module(load="imtcp")
module(load="imudp")
module(load="imrelp")
input(type="imudp" port="514")
input(type="imtcp" port="514")
input(type="imrelp" port="514")
```

The rsyslog daemon must be restarted for the changes to take effect:

```
$ sudo systemctl restart rsyslog.service
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.361 RHEL-09-652030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

All RHEL 9 remote access methods must be monitored.

```
GROUP ID: V-258144
RULE ID: SV-258144r1045286
```

Rationale:

Logging remote access methods can be used to trace the decrease in the risks associated with remote user access management. It can also be used to spot cyberattacks and ensure ongoing compliance with organizational policies surrounding the use of remote access methods.

Audit:

Verify that RHEL 9 monitors all remote access methods.
Check that remote access methods are being logged by running the following command:

```
$ grep -rE '(auth.\*|authpriv.\*|daemon.\*)' /etc/rsyslog.conf
/etc/rsyslog.d/

/etc/rsyslog.conf:authpriv.*
```

If "auth.*", "authpriv.*" or "daemon.*" are not configured to be logged, this is a finding.

Remediation:

Add or update the following lines to the "/etc/rsyslog.conf" file or a file in "/etc/rsyslog.d":

```
auth.*;authpriv.*;daemon.* /var/log/secure
```

The "rsyslog" service must be restarted for the changes to take effect with the following command:

```
$ sudo systemctl restart rsyslog.service
```

Additional Information:

CCI-000067 Employ automated mechanisms to monitor remote access methods.

- NIST SP 800-53 :: AC-17 (1)
- NIST SP 800-53 Revision 4 :: AC-17 (1)
- NIST SP 800-53 Revision 5 :: AC-17 (1)
- NIST SP 800-53A :: AC-17 (1).1

1.362 RHEL-09-652040 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must authenticate the remote logging server for offloading audit logs via rsyslog.

```
GROUP ID: V-258146
RULE ID: SV-258146r1045288
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Offloading is a common process in information systems with limited audit storage capacity.

RHEL 9 installation media provides "rsyslogd", a system utility providing support for message logging. Support for both internet and Unix domain sockets enables this utility to support both local and remote logging. Coupling this utility with "gnutls" (a secure communications library implementing the SSL, TLS and DTLS protocols) creates a method to securely encrypt and offload auditing.

"Rsyslog" supported authentication modes include: anon - anonymous authentication x509/fingerprint - certificate fingerprint authentication x509/certvalid - certificate validation only x509/name - certificate validation and subject name authentication

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Audit:

Verify RHEL 9 authenticates the remote logging server for offloading audit logs with the following command:

```
$ grep -i 'StreamDriver[\.]*AuthMode' /etc/rsyslog.conf /etc/rsyslog.d/*.conf

/etc/rsyslog.conf:$ActionSendStreamDriverAuthMode x509/name
```

If the variable name "StreamDriverAuthMode" is present in an omfwd statement block, this is not a finding. However, if the "StreamDriverAuthMode" variable is in a module block, this is a finding.
If the value of the "$ActionSendStreamDriverAuthMode or StreamDriver.AuthMode" option is not set to "x509/name" or the line is commented out, ask the system administrator (SA) to indicate how the audit logs are offloaded to a different system or media.
If there is no evidence that the transfer of the audit logs being offloaded to another system or media is encrypted, this is a finding.

Remediation:

Configure RHEL 9 to authenticate the remote logging server for offloading audit logs by setting the following option in "/etc/rsyslog.conf" or "/etc/rsyslog.d/[customfile].conf":

```
$ActionSendStreamDriverAuthMode x509/name
```

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4 :: AU-4 (1)
- NIST SP 800-53 Revision 5 :: AU-4 (1)

1.363 RHEL-09-652045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must encrypt the transfer of audit records offloaded onto a different system or media from the system being audited via rsyslog.

```
GROUP ID: V-258147
RULE ID: SV-258147r1045290
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Offloading is a common process in information systems with limited audit storage capacity.

RHEL 9 installation media provides "rsyslogd", a system utility providing support for message logging. Support for both internet and Unix domain sockets enables this utility to support both local and remote logging. Coupling this utility with "gnutls" (a secure communications library implementing the SSL, TLS and DTLS protocols) creates a method to securely encrypt and offload auditing.

"Rsyslog" supported authentication modes include: anon - anonymous authentication x509/fingerprint - certificate fingerprint authentication x509/certvalid - certificate validation only x509/name - certificate validation and subject name authentication

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Audit:

Verify RHEL 9 encrypts audit records offloaded onto a different system or media from the system being audited via rsyslog with the following command:

```
$ grep -i 'StreamDriver[\.]*Mode' /etc/rsyslog.conf /etc/rsyslog.d/*.conf

/etc/rsyslog.conf:$ActionSendStreamDriverMode 1
```

If the value of the "$ActionSendStreamDriverMode or StreamDriver.Mode" option is not set to "1" or the line is commented out, this is a finding.
If the variable name "StreamDriverAuthMode" is present in an omfwd statement block, this is not a finding. However, if the "StreamDriverAuthMode" variable is in a module block, this is a finding.

Remediation:

Configure RHEL 9 to encrypt offloaded audit records via rsyslog by setting the following options in "/etc/rsyslog.conf" or "/etc/rsyslog.d/[customfile].conf":

```
$ActionSendStreamDriverMode 1
```

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4 :: AU-4 (1)
- NIST SP 800-53 Revision 5 :: AU-4 (1)

1.364 RHEL-09-652050 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must encrypt via the gtls driver the transfer of audit records offloaded onto a different system or media from the system being audited via rsyslog.

```
GROUP ID: V-258148
RULE ID: SV-258148r1045292
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Offloading is a common process in information systems with limited audit storage capacity.

RHEL 9 installation media provides "rsyslogd", a system utility providing support for message logging. Support for both internet and Unix domain sockets enables this utility to support both local and remote logging. Coupling this utility with "gnutls" (a secure communications library implementing the SSL, TLS and DTLS protocols) creates a method to securely encrypt and offload auditing.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Audit:

Verify RHEL 9 uses the gtls driver to encrypt audit records offloaded onto a different system or media from the system being audited with the following command:

```
$ grep -Ei 'DefaultNetStreamDriver\b|StreamDriver.Name' /etc/rsyslog.conf
/etc/rsyslog.d/*.conf

/etc/rsyslog.conf:$DefaultNetstreamDriver gtls
```

If the value of the "$DefaultNetstreamDriver or StreamDriver" option is not set to "gtls" or the line is commented out, this is a finding.
If the variable name "StreamDriver" is present in an omfwd statement block, this is not a finding. However, if the "StreamDriver" variable is in a module block, this is a finding.

Remediation:

Configure RHEL 9 to use the gtls driver to encrypt offloaded audit records by setting the following options in "/etc/rsyslog.conf" or "/etc/rsyslog.d/[customfile].conf":

```
$DefaultNetstreamDriver gtls
```

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4 :: AU-4 (1)
- NIST SP 800-53 Revision 5 :: AU-4 (1)

1.365 RHEL-09-652055 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must be configured to forward audit records via TCP to a different system or media from the system being audited via rsyslog.

```
GROUP ID: V-258149
RULE ID: SV-258149r1045294
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Offloading is a common process in information systems with limited audit storage capacity.

RHEL 9 installation media provides "rsyslogd", a system utility providing support for message logging. Support for both internet and Unix domain sockets enables this utility to support both local and remote logging. Coupling this utility with "gnutls" (a secure communications library implementing the SSL, TLS and DTLS protocols) creates a method to securely encrypt and offload auditing.

Rsyslog provides three ways to forward message: the traditional UDP transport, which is extremely lossy but standard; the plain TCP based transport, which loses messages only during certain situations but is widely available; and the RELP transport, which does not lose messages but is currently available only as part of the rsyslogd 3.15.0 and above.

Examples of each configuration: UDP *.* @remotesystemname TCP *.* @@remotesystemname RELP *.* :omrelp:remotesystemname:2514 Note that a port number was given as there is no standard port for RELP.

Satisfies: SRG-OS-000479-GPOS-00224, SRG-OS-000480-GPOS-00227, SRG-OS-000342-GPOS-00133

Audit:

Verify that RHEL 9 audit system offloads audit records onto a different system or media from the system being audited via rsyslog using TCP with the following command:

```
$ grep -i 'type="omfwd"' /etc/rsyslog.conf /etc/rsyslog.d/*.conf

*.* action(type="omfwd" target="[remoteloggingserver]" protocol="tcp"
port="[port]"
```

If a remote server is not configured, or the line is commented out, ask the system administrator (SA) to indicate how the audit logs are offloaded to a different system or media.
If there is no evidence that the audit logs are being offloaded to another system or media, this is a finding.

Remediation:

Configure RHEL 9 to offload audit records onto a different system or media from the system being audited via TCP using rsyslog by specifying the remote logging server in "/etc/rsyslog.conf"" or "/etc/rsyslog.d/[customfile].conf" with the name or IP address of the log aggregation server.

```
*.* @@[remoteloggingserver]:[port]"
```

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4 :: AU-4 (1)
- NIST SP 800-53 Revision 5 :: AU-4 (1)

1.366 RHEL-09-652060 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must use cron logging.

```
GROUP ID: V-258150
RULE ID: SV-258150r1045296
```

Rationale:

Cron logging can be used to trace the successful or unsuccessful execution of cron jobs. It can also be used to spot intrusions into the use of the cron facility by unauthorized and malicious users.

Audit:

Verify that "rsyslog" is configured to log cron events with the following command:
Note: If another logging package is used, substitute the utility configuration file for "/etc/rsyslog.conf" or "/etc/rsyslog.d/*.conf" files.

```
$ grep -s cron /etc/rsyslog.conf /etc/rsyslog.d/*.conf

/etc/rsyslog.conf:*.info;mail.none;authpriv.none;cron.none /var/log/messages
/etc/rsyslog.conf:cron.* /var/log/cron
```

If the command does not return a response, check for cron logging all facilities with the following command:

```
$ logger -p local0.info "Test message for all facilities."
```

Check the logs for the test message with:

```
$ sudo tail /var/log/messages
```

If "rsyslog" is not logging messages for the cron facility or all facilities, this is a finding.

Remediation:

Configure "rsyslog" to log all cron messages by adding or updating the following line to "/etc/rsyslog.conf" or a configuration file in the /etc/rsyslog.d/ directory:

```
cron.* /var/log/cron
```

The rsyslog daemon must be restarted for the changes to take effect:

```
$ sudo systemctl restart rsyslog.service
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.367 RHEL-09-653010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 audit package must be installed.

```
GROUP ID: V-258151
RULE ID: SV-258151r1045298
```

Rationale:

Without establishing what type of events occurred, the source of events, where events occurred, and the outcome of events, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Associating event types with detected events in audit logs provides a means of investigating an attack, recognizing resource utilization or capacity thresholds, or identifying an improperly configured RHEL 9 system.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000040-GPOS-00018, SRG-OS-000041-GPOS-00019, SRG-OS-000042-GPOS-00021, SRG-OS-000051-GPOS-00024, SRG-OS-000054-GPOS-00025, SRG-OS-000122-GPOS-00063, SRG-OS-000254-GPOS-00095, SRG-OS-000255-GPOS-00096, SRG-OS-000337-GPOS-00129, SRG-OS-000348-GPOS-00136, SRG-OS-000349-GPOS-00137, SRG-OS-000350-GPOS-00138, SRG-OS-000351-GPOS-00139, SRG-OS-000352-GPOS-00140, SRG-OS-000353-GPOS-00141, SRG-OS-000354-GPOS-00142, SRG-OS-000358-GPOS-00145, SRG-OS-000365-GPOS-00152, SRG-OS-000392-GPOS-00172, SRG-OS-000475-GPOS-00220, SRG-OS-000055-GPOS-00026

Audit:

Verify that the RHEL 9 audit service package is installed.
Check that the audit service package is installed with the following command:

```
$ dnf list --installed audit
```

Example output:

```
audit-3.0.7-101.el9_0.2.x86_64
```

If the "audit" package is not installed, this is a finding.

Remediation:

Install the audit service package (if the audit service is not already installed) with the following command:

```
$ sudo dnf install audit
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000131 Ensure that audit records containing information that establishes when the event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 b
- NIST SP 800-53A :: AU-3.1

CCI-000132 Ensure that audit records containing information that establishes where the event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 c
- NIST SP 800-53A :: AU-3.1

CCI-000133 Ensure that audit records containing information that establishes the source of the event.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 d
- NIST SP 800-53A :: AU-3.1

CCI-000134 Ensure that audit records containing information that establishes the outcome of the event.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 e
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000154 Provide the capability to centrally review and analyze audit records from multiple components within the system.

- NIST SP 800-53 :: AU-6 (4)
- NIST SP 800-53 Revision 4 :: AU-6 (4)
- NIST SP 800-53 Revision 5 :: AU-6 (4)
- NIST SP 800-53A :: AU-6 (4).1

CCI-000158 Provide the capability to process, sort, and search audit records for events of interest based on organization-defined audit fields within audit records.

- NIST SP 800-53 :: AU-7 (1)
- NIST SP 800-53 Revision 4 :: AU-7 (1)
- NIST SP 800-53 Revision 5 :: AU-7 (1)
- NIST SP 800-53A :: AU-7 (1).1

CCI-000159 Use internal system clocks to generate time stamps for audit records.

- NIST SP 800-53 :: AU-8
- NIST SP 800-53 Revision 4 :: AU-8 a
- NIST SP 800-53 Revision 5 :: AU-8 a
- NIST SP 800-53A :: AU-8.1

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-001464 Initiates session audits automatically at system start-up.

- NIST SP 800-53 :: AU-14 (1)
- NIST SP 800-53 Revision 4 :: AU-14 (1)
- NIST SP 800-53 Revision 5 :: AU-14 (1)
- NIST SP 800-53A :: AU-14 (1).1

CCI-001487 Ensure that audit records containing information that establishes the identity of any individuals, subjects, or objects/entities associated with the event.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 f
- NIST SP 800-53A :: AU-3.1

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5 :: CM-5 (1) (b)

CCI-001875 Provide an audit reduction capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001876 Provide an audit reduction capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001877 Provide an audit reduction capability that supports after-the-fact investigations of incidents.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001878 Provide a report generation capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001879 Provide a report generation capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001880 Provide a report generation capability that supports after-the-fact investigations of security incidents.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001881 Provide an audit reduction capability that does not alter original content or time ordering of audit records.

- NIST SP 800-53 Revision 4 :: AU-7 b
- NIST SP 800-53 Revision 5 :: AU-7 b

CCI-001882 Provide a report generation capability that does not alter original content or time ordering of audit records.

- NIST SP 800-53 Revision 4 :: AU-7 b
- NIST SP 800-53 Revision 5 :: AU-7 b

CCI-001889 Record time stamps for audit records that meet organization-defined granularity of time measurement.

- NIST SP 800-53 Revision 4 :: AU-8 b
- NIST SP 800-53 Revision 5 :: AU-8 b

CCI-001914 Provide the capability for organization-defined individuals or roles to change the logging to be performed on organization-defined system components based on organization-defined selectable event criteria within organization-defined time thresholds.

- NIST SP 800-53 Revision 4 :: AU-12 (3)
- NIST SP 800-53 Revision 5 :: AU-12 (3)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

CCI-001814 The Information system supports auditing of the enforcement actions.

- NIST SP 800-53 Revision 4 :: CM-5 (1)

1.368 RHEL-09-653015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 audit service must be enabled.

```
GROUP ID: V-258152
RULE ID: SV-258152r1015127
```

Rationale:

Without establishing what type of events occurred, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack. Ensuring the "auditd" service is active ensures audit records generated by the kernel are appropriately recorded.

Additionally, a properly configured audit subsystem ensures that actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000037-GPOS-00015, SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000040-GPOS-00018, SRG-OS-000041-GPOS-00019, SRG-OS-000042-GPOS-00021, SRG-OS-000051-GPOS-00024, SRG-OS-000054-GPOS-00025, SRG-OS-000122-GPOS-00063, SRG-OS-000254-GPOS-00095, SRG-OS-000255-GPOS-00096, SRG-OS-000337-GPOS-00129, SRG-OS-000348-GPOS-00136, SRG-OS-000349-GPOS-00137, SRG-OS-000350-GPOS-00138, SRG-OS-000351-GPOS-00139, SRG-OS-000352-GPOS-00140, SRG-OS-000353-GPOS-00141, SRG-OS-000354-GPOS-00142, SRG-OS-000358-GPOS-00145, SRG-OS-000365-GPOS-00152, SRG-OS-000392-GPOS-00172, SRG-OS-000475-GPOS-00220

Audit:

Verify the audit service is configured to produce audit records with the following command:

```
$ systemctl status auditd.service

auditd.service - Security Auditing Service
Loaded:loaded (/usr/lib/systemd/system/auditd.service; enabled; vendor
preset: enabled)
Active: active (running) since Tues 2022-05-24 12:56:56 EST; 4 weeks 0 days
ago
```

If the audit service is not "active" and "running", this is a finding.

Remediation:

To enable the auditd service run the following command:

```
$ sudo systemctl enable --now auditd
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000131 Ensure that audit records containing information that establishes when the event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 b
- NIST SP 800-53A :: AU-3.1

CCI-000132 Ensure that audit records containing information that establishes where the event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 c
- NIST SP 800-53A :: AU-3.1

CCI-000133 Ensure that audit records containing information that establishes the source of the event.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 d
- NIST SP 800-53A :: AU-3.1

CCI-000134 Ensure that audit records containing information that establishes the outcome of the event.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 e
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000154 Provide the capability to centrally review and analyze audit records from multiple components within the system.

- NIST SP 800-53 :: AU-6 (4)
- NIST SP 800-53 Revision 4 :: AU-6 (4)
- NIST SP 800-53 Revision 5 :: AU-6 (4)
- NIST SP 800-53A :: AU-6 (4).1

CCI-000158 Provide the capability to process, sort, and search audit records for events of interest based on organization-defined audit fields within audit records.

- NIST SP 800-53 :: AU-7 (1)
- NIST SP 800-53 Revision 4 :: AU-7 (1)
- NIST SP 800-53 Revision 5 :: AU-7 (1)
- NIST SP 800-53A :: AU-7 (1).1

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-001464 Initiates session audits automatically at system start-up.

- NIST SP 800-53 :: AU-14 (1)
- NIST SP 800-53 Revision 4 :: AU-14 (1)
- NIST SP 800-53 Revision 5 :: AU-14 (1)
- NIST SP 800-53A :: AU-14 (1).1

CCI-001487 Ensure that audit records containing information that establishes the identity of any individuals, subjects, or objects/entities associated with the event.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 f
- NIST SP 800-53A :: AU-3.1

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5 :: CM-5 (1) (b)

CCI-001875 Provide an audit reduction capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001876 Provide an audit reduction capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001877 Provide an audit reduction capability that supports after-the-fact investigations of incidents.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001878 Provide a report generation capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001879 Provide a report generation capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001880 Provide a report generation capability that supports after-the-fact investigations of security incidents.

- NIST SP 800-53 Revision 4 :: AU-7 a
- NIST SP 800-53 Revision 5 :: AU-7 a

CCI-001881 Provide an audit reduction capability that does not alter original content or time ordering of audit records.

- NIST SP 800-53 Revision 4 :: AU-7 b
- NIST SP 800-53 Revision 5 :: AU-7 b

CCI-001882 Provide a report generation capability that does not alter original content or time ordering of audit records.

- NIST SP 800-53 Revision 4 :: AU-7 b
- NIST SP 800-53 Revision 5 :: AU-7 b

CCI-001889 Record time stamps for audit records that meet organization-defined granularity of time measurement.

- NIST SP 800-53 Revision 4 :: AU-8 b
- NIST SP 800-53 Revision 5 :: AU-8 b

CCI-001914 Provide the capability for organization-defined individuals or roles to change the logging to be performed on organization-defined system components based on organization-defined selectable event criteria within organization-defined time thresholds.

- NIST SP 800-53 Revision 4 :: AU-12 (3)
- NIST SP 800-53 Revision 5 :: AU-12 (3)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

CCI-004188 Monitor the use of maintenance tools that execute with increased privilege.

- NIST SP 800-53 Revision 5 :: MA-3 (5)

CCI-001814 The Information system supports auditing of the enforcement actions.

- NIST SP 800-53 Revision 4 :: CM-5 (1)

1.369 RHEL-09-653020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 audit system must take appropriate action when an error writing to the audit storage volume occurs.

```
GROUP ID: V-258153
RULE ID: SV-258153r1038966
```

Rationale:

It is critical that when the operating system is at risk of failing to process audit logs as required, it takes action to mitigate the failure. Audit processing failures include software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded. Responses to audit failure depend upon the nature of the failure mode.

Audit:

Verify RHEL 9 takes the appropriate action when an audit processing failure occurs. Check that RHEL 9 takes the appropriate action when an audit processing failure occurs with the following command:

```
$ sudo grep disk_error_action /etc/audit/auditd.conf

disk_error_action = HALT
```

If the value of the "disk_error_action" option is not "SYSLOG", "SINGLE", or "HALT", or the line is commented out, ask the system administrator (SA) to indicate how the system takes appropriate action when an audit process failure occurs. If there is no evidence of appropriate action, this is a finding.

Remediation:

Configure RHEL 9 to shut down by default upon audit failure (unless availability is an overriding concern).
Add or update the following line (depending on configuration "disk_error_action" can be set to "SYSLOG" or "SINGLE" depending on configuration) in "/etc/audit/auditd.conf" file:

```
disk_error_action = HALT
```

If availability has been determined to be more important, and this decision is documented with the information system security officer (ISSO), configure the operating system to notify SA staff and ISSO staff in the event of an audit processing failure by setting the "disk_error_action" to "SYSLOG".

Additional Information:

CCI-000140 Take organization-defined actions upon audit failure include, shutting down the system, overwriting oldest audit records, and stopping the generation of audit records.

- NIST SP 800-53 :: AU-5 b
- NIST SP 800-53 Revision 4 :: AU-5 b
- NIST SP 800-53 Revision 5 :: AU-5 b
- NIST SP 800-53A :: AU-5.1 (iv)

1.370 RHEL-09-653025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 audit system must take appropriate action when the audit storage volume is full.

```
GROUP ID: V-258154
RULE ID: SV-258154r1038966
```

Rationale:

It is critical that when the operating system is at risk of failing to process audit logs as required, it takes action to mitigate the failure. Audit processing failures include software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded. Responses to audit failure depend upon the nature of the failure mode.

Audit:

Verify RHEL 9 takes the appropriate action when the audit storage volume is full.
Check that RHEL 9 takes the appropriate action when the audit storage volume is full with the following command:

```
$ sudo grep disk_full_action /etc/audit/auditd.conf

disk_full_action = HALT
```

If the value of the "disk_full_action" option is not "SYSLOG", "SINGLE", or "HALT", or the line is commented out, ask the system administrator (SA) to indicate how the system takes appropriate action when an audit storage volume is full. If there is no evidence of appropriate action, this is a finding.

Remediation:

Configure RHEL 9 to shut down by default upon audit failure (unless availability is an overriding concern).
Add or update the following line (depending on configuration "disk_full_action" can be set to "SYSLOG" or "SINGLE" depending on configuration) in "/etc/audit/auditd.conf" file:

```
disk_full_action = HALT
```

If availability has been determined to be more important, and this decision is documented with the information system security officer (ISSO), configure the operating system to notify SA staff and ISSO staff in the event of an audit processing failure by setting the "disk_full_action" to "SYSLOG".

Additional Information:

CCI-000140 Take organization-defined actions upon audit failure include, shutting down the system, overwriting oldest audit records, and stopping the generation of audit records.

- NIST SP 800-53 :: AU-5 b
- NIST SP 800-53 Revision 4 :: AU-5 b
- NIST SP 800-53 Revision 5 :: AU-5 b
- NIST SP 800-53A :: AU-5.1 (iv)

1.371 RHEL-09-653030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must allocate audit record storage capacity to store at least one week's worth of audit records.

```
GROUP ID: V-258155
RULE ID: SV-258155r1045300
```

Rationale:

To ensure RHEL 9 systems have a sufficient storage capacity in which to write the audit logs, RHEL 9 needs to be able to allocate audit record storage capacity.

The task of allocating audit record storage capacity is usually performed during initial installation of RHEL 9.

Satisfies: SRG-OS-000341-GPOS-00132, SRG-OS-000342-GPOS-00133

Audit:

Verify RHEL 9 allocates audit record storage capacity to store at least one week of audit records when audit records are not immediately sent to a central audit record storage facility.
Note: The partition size needed to capture a week of audit records is based on the activity level of the system and the total storage capacity available. Typically 10.0GB of storage space for audit records should be sufficient.
Determine which partition the audit records are being written to with the following command:

```
$ sudo grep -w 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 following command and verify whether it is sufficiently large:

```
# df -h /var/log/audit/

/dev/sda2 24G 10.4G 13.6G 43% /var/log/audit
```

If the audit record partition is not allocated for sufficient storage capacity, this is a finding.

Remediation:

Allocate enough storage capacity for at least one week of audit records when audit records are not immediately sent to a central audit record storage facility.
If audit records are stored on a partition made specifically for audit records, resize the partition with sufficient space to contain one week of audit records.
If audit records are not stored on a partition made specifically for audit records, a new partition with sufficient space will need be to be created.

Additional Information:

CCI-001849 Allocate audit log storage capacity to accommodate organization-defined audit record retention requirements.

- NIST SP 800-53 Revision 4 :: AU-4
- NIST SP 800-53 Revision 5 :: AU-4

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4 :: AU-4 (1)
- NIST SP 800-53 Revision 5 :: AU-4 (1)

1.372 RHEL-09-653035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must take action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity.

```
GROUP ID: V-258156
RULE ID: SV-258156r971542
```

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 RHEL 9 takes action when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity with the following command:

```
$ sudo grep -w space_left /etc/audit/auditd.conf

space_left = 25%
```

If the value of the "space_left" keyword is not set to 25 percent of the storage volume allocated to audit logs, or if the line is commented out, ask the system administrator (SA) to indicate how the system is providing real-time alerts to the SA and information system security officer (ISSO). If the "space_left" value is not configured to the correct value, this is a finding.

Remediation:

Configure RHEL 9 to initiate an action to notify the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity by adding/modifying the following line in the /etc/audit/auditd.conf file.

```
space_left  = 25%
```

Additional Information:

CCI-001855 Provide a warning to organization-defined personnel, roles, and/or locations within an organization-defined time period when allocated audit log storage volume reaches an organization-defined percentage of repository maximum audit log storage capacity.

- NIST SP 800-53 Revision 4 :: AU-5 (1)
- NIST SP 800-53 Revision 5 :: AU-5 (1)

1.373 RHEL-09-653040 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must notify the system administrator (SA) and information system security officer (ISSO) (at a minimum) when allocated audit record storage volume 75 percent utilization.

```
GROUP ID: V-258157
RULE ID: SV-258157r971542
```

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 RHEL 9 notifies the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity with the following command:

```
$ sudo grep -w space_left_action /etc/audit/auditd.conf

space_left_action = email
```

If the value of the "space_left_action" is not set to "email", or if the line is commented out, ask the SA to indicate how the system is providing real-time alerts to the SA and ISSO.
If there is no evidence that real-time alerts are configured on the system, this is a finding.

Remediation:

Configure RHEL 9 to initiate an action to notify the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity by adding/modifying the following line in the /etc/audit/auditd.conf file.

```
space_left_action = email
```

Additional Information:

CCI-001855 Provide a warning to organization-defined personnel, roles, and/or locations within an organization-defined time period when allocated audit log storage volume reaches an organization-defined percentage of repository maximum audit log storage capacity.

- NIST SP 800-53 Revision 4 :: AU-5 (1)
- NIST SP 800-53 Revision 5 :: AU-5 (1)

1.374 RHEL-09-653045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must take action when allocated audit record storage volume reaches 95 percent of the audit record storage capacity.

```
GROUP ID: V-258158
RULE ID: SV-258158r971542
```

Rationale:

If action is not taken when storage volume reaches 95 percent utilization, the auditing system may fail when the storage volume reaches capacity.

Audit:

Verify RHEL 9 takes action when allocated audit record storage volume reaches 95 percent of the repository maximum audit record storage capacity with the following command:

```
$ sudo grep -w admin_space_left /etc/audit/auditd.conf

admin_space_left = 5%
```

If the value of the "admin_space_left" keyword is not set to 5 percent of the storage volume allocated to audit logs, or if the line is commented out, ask the system administrator (SA) to indicate how the system is taking action if the allocated storage is about to reach capacity. If the "space_left" value is not configured to the correct value, this is a finding.

Remediation:

Configure RHEL 9 to initiate an action when allocated audit record storage volume reaches 95 percent of the repository maximum audit record storage capacity by adding/modifying the following line in the /etc/audit/auditd.conf file.

```
admin_space_left  = 5%
```

Additional Information:

CCI-001855 Provide a warning to organization-defined personnel, roles, and/or locations within an organization-defined time period when allocated audit log storage volume reaches an organization-defined percentage of repository maximum audit log storage capacity.

- NIST SP 800-53 Revision 4 :: AU-5 (1)
- NIST SP 800-53 Revision 5 :: AU-5 (1)

1.375 RHEL-09-653050 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must take action when allocated audit record storage volume reaches 95 percent of the repository maximum audit record storage capacity.

```
GROUP ID: V-258159
RULE ID: SV-258159r971542
```

Rationale:

If action is not taken when storage volume reaches 95 percent utilization, the auditing system may fail when the storage volume reaches capacity.

Audit:

Verify that RHEL 9 is configured to take action in the event of allocated audit record storage volume reaches 95 percent of the repository maximum audit record storage capacity with the following command:

```
$ sudo grep admin_space_left_action /etc/audit/auditd.conf

admin_space_left_action = single
```

If the value of the "admin_space_left_action" is not set to "single", or if the line is commented out, ask the system administrator (SA) to indicate how the system is providing real-time alerts to the SA and information system security officer (ISSO).
If there is no evidence that real-time alerts are configured on the system, this is a finding.

Remediation:

Configure "auditd" service to take action in the event of allocated audit record storage volume reaches 95 percent of the repository maximum audit record storage capacity.
Edit the following line in "/etc/audit/auditd.conf" to ensure that the system is forced into single user mode in the event the audit record storage volume is about to reach maximum capacity:

```
admin_space_left_action = single
```

The audit daemon must be restarted for changes to take effect.

Additional Information:

CCI-001855 Provide a warning to organization-defined personnel, roles, and/or locations within an organization-defined time period when allocated audit log storage volume reaches an organization-defined percentage of repository maximum audit log storage capacity.

- NIST SP 800-53 Revision 4 :: AU-5 (1)
- NIST SP 800-53 Revision 5 :: AU-5 (1)

1.376 RHEL-09-653055 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 audit system must take appropriate action when the audit files have reached maximum size.

```
GROUP ID: V-258160
RULE ID: SV-258160r1038966
```

Rationale:

It is critical that when the operating system is at risk of failing to process audit logs as required, it takes action to mitigate the failure. Audit processing failures include software/hardware errors; failures in the audit capturing mechanisms; and audit storage capacity being reached or exceeded. Responses to audit failure depend upon the nature of the failure mode.

Audit:

Verify that RHEL 9 takes the appropriate action when the audit files have reached maximum size with the following command:

```
$ sudo grep max_log_file_action /etc/audit/auditd.conf

max_log_file_action = ROTATE
```

If the value of the "max_log_file_action" option is not "ROTATE", "SINGLE", or the line is commented out, ask the system administrator (SA)to indicate how the system takes appropriate action when an audit storage volume is full. If there is no evidence of appropriate action, this is a finding.

Remediation:

Configure RHEL 9 to rotate the audit log when it reaches maximum size.
Add or update the following line in "/etc/audit/auditd.conf" file:

```
max_log_file_action = ROTATE
```

Additional Information:

CCI-000140 Take organization-defined actions upon audit failure include, shutting down the system, overwriting oldest audit records, and stopping the generation of audit records.

- NIST SP 800-53 :: AU-5 b
- NIST SP 800-53 Revision 4 :: AU-5 b
- NIST SP 800-53 Revision 5 :: AU-5 b
- NIST SP 800-53A :: AU-5.1 (iv)

1.377 RHEL-09-653060 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must label all offloaded audit logs before sending them to the central log server.

```
GROUP ID: V-258161
RULE ID: SV-258161r958416
```

Rationale:

Enriched logging is needed to determine who, what, and when events occur on a system. Without this, determining root cause of an event will be much more difficult.

When audit logs are not labeled before they are sent to a central log server, the audit data will not be able to be analyzed and tied back to the correct system.

Satisfies: SRG-OS-000039-GPOS-00017, SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Audit:

Verify that RHEL 9 Audit Daemon is configured to label all offloaded audit logs, with the following command:

```
$ sudo grep name_format /etc/audit/auditd.conf

name_format = hostname
```

If the "name_format" option is not "hostname", "fqd", or "numeric", or the line is commented out, this is a finding.

Remediation:

Edit the /etc/audit/auditd.conf file and add or update the "name_format" option:

```
name_format = hostname
```

The audit daemon must be restarted for changes to take effect.

Additional Information:

CCI-000132 Ensure that audit records containing information that establishes where the event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 c
- NIST SP 800-53A :: AU-3.1

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4 :: AU-4 (1)
- NIST SP 800-53 Revision 5 :: AU-4 (1)

1.378 RHEL-09-653065 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must take appropriate action when the internal event queue is full.

```
GROUP ID: V-258162
RULE ID: SV-258162r958754
```

Rationale:

The audit system should have an action setup in the event the internal event queue becomes full so that no data is lost. Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Offloading is a common process in information systems with limited audit storage capacity.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Audit:

Verify that RHEL 9 audit system is configured to take an appropriate action when the internal event queue is full:

```
$ sudo grep -i overflow_action /etc/audit/auditd.conf

overflow_action = syslog
```

If the value of the "overflow_action" option is not set to "syslog", "single", "halt" or the line is commented out, ask the system administrator (SA) to indicate how the audit logs are offloaded to a different system or media.
If there is no evidence that the transfer of the audit logs being offloaded to another system or media takes appropriate action if the internal event queue becomes full, this is a finding.

Remediation:

Edit the /etc/audit/auditd.conf file and add or update the "overflow_action" option:

```
overflow_action = syslog
```

The audit daemon must be restarted for changes to take effect.

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4 :: AU-4 (1)
- NIST SP 800-53 Revision 5 :: AU-4 (1)

1.379 RHEL-09-653070 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 System Administrator (SA) and/or information system security officer (ISSO) (at a minimum) must be alerted of an audit processing failure event.

```
GROUP ID: V-258163
RULE ID: SV-258163r958424
```

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.

Satisfies: SRG-OS-000046-GPOS-00022, SRG-OS-000343-GPOS-00134

Audit:

Verify that RHEL 9 is configured to notify the SA and/or ISSO (at a minimum) in the event of an audit processing failure with the following command:

```
$ sudo grep action_mail_acct /etc/audit/auditd.conf

action_mail_acct = root
```

If the value of the "action_mail_acct" keyword is not set to "root" and/or other accounts for security personnel, the "action_mail_acct" keyword is missing, or the retuned line is commented out, ask the SA to indicate how they and the ISSO are notified of an audit process failure. If there is no evidence of the proper personnel being notified of an audit processing failure, this is a finding.

Remediation:

Configure "auditd" service to notify the SA and ISSO in the event of an audit processing failure.
Edit the following line in "/etc/audit/auditd.conf" to ensure that administrators are notified via email for those situations:

```
action_mail_acct = root
```

The audit daemon must be restarted for changes to take effect.

Additional Information:

CCI-000139 Alert organization-defined personnel or roles within an organization-defined time period in the event of an audit logging process failure.

- NIST SP 800-53 :: AU-5 a
- NIST SP 800-53 Revision 4 :: AU-5 a
- NIST SP 800-53 Revision 5 :: AU-5 a
- NIST SP 800-53A :: AU-5.1 (ii)

CCI-001855 Provide a warning to organization-defined personnel, roles, and/or locations within an organization-defined time period when allocated audit log storage volume reaches an organization-defined percentage of repository maximum audit log storage capacity.

- NIST SP 800-53 Revision 4 :: AU-5 (1)
- NIST SP 800-53 Revision 5 :: AU-5 (1)

1.380 RHEL-09-653075 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 audit system must audit local events.

```
GROUP ID: V-258164
RULE ID: SV-258164r1045301
```

Rationale:

Without establishing what type of events occurred, the source of events, where events occurred, and the outcome of events, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

If option "local_events" isn't set to "yes" only events from network will be aggregated.

Satisfies: SRG-OS-000062-GPOS-00031, SRG-OS-000480-GPOS-00227

Audit:

Verify that the RHEL 9 audit system is configured to audit local events with the following command:

```
$ sudo grep local_events /etc/audit/auditd.conf

local_events = yes
```

If "local_events" isn't set to "yes", if the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records for local events by adding or updating the following line in "/etc/audit/auditd.conf":

```
local_events = yes
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

1.381 RHEL-09-653080 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 audit logs must be group-owned by root or by a restricted logging group to prevent unauthorized read access.

```
GROUP ID: V-258165
RULE ID: SV-258165r958434
```

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029, SRG-OS-000206-GPOS-00084

Audit:

Verify the audit logs are group-owned by "root" or a restricted logging group.
First determine if a group other than "root" has been assigned to the audit logs with the following command:

```
$ sudo grep log_group /etc/audit/auditd.conf
```

Then determine where the audit logs are stored with the following command:

```
$ sudo grep -iw log_file /etc/audit/auditd.conf

log_file = /var/log/audit/audit.log
```

Then using the location of the audit log file, determine if the audit log is group-owned by "root" using the following command:

```
$ sudo stat -c "%G %n" /var/log/audit/audit.log

root /var/log/audit/audit.log
```

If the audit log is not group-owned by "root" or the configured alternative logging group, this is a finding.

Remediation:

Change the group of the directory of "/var/log/audit" to be owned by a correct group. Identify the group that is configured to own audit log:

```
$ sudo grep -P '^[ ]*log_group[ ]+=.*$' /etc/audit/auditd.conf
```

Change the ownership to that group:

```
$ sudo chgrp ${GROUP} /var/log/audit
```

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

1.382 RHEL-09-653085 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 audit log directory must be owned by root to prevent unauthorized read access.

```
GROUP ID: V-258166
RULE ID: SV-258166r1045303
```

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029, SRG-OS-000206-GPOS-00084

Audit:

Verify the audit logs directory is owned by "root".
Determine where the audit logs are stored with the following command:

```
$ sudo grep -iw log_file /etc/audit/auditd.conf

log_file = /var/log/audit/audit.log
```

Using the location of the audit log file, determine if the audit log directory is owned by "root" using the following command:

```
$ sudo stat -c '%U %n' /var/log/audit

root /var/log/audit
```

If the audit log directory is not owned by "root", this is a finding.

Remediation:

Configure the audit log to be protected from unauthorized read access by setting the correct owner as "root" with the following command:

```
$ sudo chown root /var/log/audit
```

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

1.383 RHEL-09-653090 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 audit logs file must have mode 0600 or less permissive to prevent unauthorized access to the audit log.

```
GROUP ID: V-258167
RULE ID: SV-258167r1045306
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the RHEL 9 system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029, SRG-OS-000206-GPOS-00084

Audit:

Verify the audit logs have a mode of "0600".
Determine where the audit logs are stored with the following command:

```
$ sudo grep -iw log_file /etc/audit/auditd.conf

log_file = /var/log/audit/audit.log
```

Using the location of the audit log file, determine the mode of each audit log with the following command:

```
$ sudo find /var/log/audit/ -type f -exec stat -c '%a %n' {} \;

rw-------. 2 root root 237923 Jun 11 11:56 /var/log/audit/audit.log
```

If the audit logs have a mode more permissive than "0600", this is a finding.

Remediation:

Configure the audit logs to have a mode of "0600" with the following command: Replace "[audit_log_file]" with the path to each audit log file. By default, these logs are located in "/var/log/audit/.

```
$ sudo chmod 0600 /var/log/audit/[audit_log_file]
```

Check the group that owns the system audit logs:

```
$ sudo grep -iw log_group /etc/audit/auditd.conf
```

If log_group is set to a user other than root, configure the permissions the following way:

```
$ sudo chmod 0640 $log_file
$ sudo chmod 0440 $log_file.*
```

Otherwise, configure the permissions the following way:

```
$ sudo chmod 0600 $log_file
$ sudo chmod 0400 $log_file.*
```

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53 :: SI-11 c
- NIST SP 800-53 Revision 4 :: SI-11 b
- NIST SP 800-53 Revision 5 :: SI-11 b
- NIST SP 800-53A :: SI-11.1 (iv)

1.384 RHEL-09-653095 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must periodically flush audit records to disk to prevent the loss of audit records.

```
GROUP ID: V-258168
RULE ID: SV-258168r958428
```

Rationale:

If option "freq" is not set to a value that requires audit records being written to disk after a threshold number is reached, then audit records may be lost.

Audit:

Verify that audit system is configured to flush to disk after every 100 records with the following command:

```
$ sudo grep freq /etc/audit/auditd.conf

freq = 100
```

If "freq" isn't set to a value between "1" and "100", the value is missing, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to flush audit to disk by adding or updating the following rule in "/etc/audit/auditd.conf":

```
freq = 100
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

CCI-000154 Provide the capability to centrally review and analyze audit records from multiple components within the system.

- NIST SP 800-53 :: AU-6 (4)
- NIST SP 800-53 Revision 4 :: AU-6 (4)
- NIST SP 800-53 Revision 5 :: AU-6 (4)
- NIST SP 800-53A :: AU-6 (4).1

1.385 RHEL-09-653100 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must produce audit records containing information to establish the identity of any individual or process associated with the event.

```
GROUP ID: V-258169
RULE ID: SV-258169r991556
```

Rationale:

Without establishing what type of events occurred, the source of events, where events occurred, and the outcome of events, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Enriched logging aids in making sense of who, what, and when events occur on a system. Without this, determining root cause of an event will be much more difficult.

Satisfies: SRG-OS-000255-GPOS-00096, SRG-OS-000480-GPOS-00227

Audit:

Verify that RHEL 9 audit system is configured to resolve audit information before writing to disk, with the following command:

```
$ sudo grep log_format /etc/audit/auditd.conf

log_format = ENRICHED
```

If the "log_format" option is not "ENRICHED", or the line is commented out, this is a finding.

Remediation:

Edit the /etc/audit/auditd.conf file and add or update the "log_format" option:

```
log_format = ENRICHED
```

The audit daemon must be restarted for changes to take effect.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

CCI-001487 Ensure that audit records containing information that establishes the identity of any individuals, subjects, or objects/entities associated with the event.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 f
- NIST SP 800-53A :: AU-3.1

1.386 RHEL-09-653105 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must write audit records to disk.

```
GROUP ID: V-258170
RULE ID: SV-258170r991589
```

Rationale:

Audit data should be synchronously written to disk to ensure log integrity. This setting assures that all audit event data is written disk.

Audit:

Verify that the audit system is configured to write logs to the disk with the following command:

```
$ sudo grep write_logs /etc/audit/auditd.conf

write_logs = yes
```

If "write_logs" does not have a value of "yes", the line is commented out, or the line is missing, this is a finding.

Remediation:

Configure the audit system to write log files to the disk.
Edit the /etc/audit/auditd.conf file and add or update the "write_logs" option to "yes":

```
write_logs = yes
```

The audit daemon must be restarted for changes to take effect.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53 :: CM-6 b
- NIST SP 800-53 Revision 4 :: CM-6 b
- NIST SP 800-53 Revision 5 :: CM-6 b
- NIST SP 800-53A :: CM-6.1 (iv)

1.387 RHEL-09-653110 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must allow only the information system security manager (ISSM) (or individuals or roles appointed by the ISSM) to select which auditable events are to be audited.

```
GROUP ID: V-258171
RULE ID: SV-258171r1045308
```

Rationale:

Without the capability to restrict the roles and individuals that can select which events are audited, unauthorized personnel may be able to prevent the auditing of critical events. Misconfigured audits may degrade the system's performance by overwhelming the audit log. Misconfigured audits may also make it more difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit:

Verify that the files in directory "/etc/audit/rules.d/" and "/etc/audit/auditd.conf" file have a mode of "0640" or less permissive with the following command:

```
$ sudo find /etc/audit/rules.d/ /etc/audit/audit.rules /etc/audit/auditd.conf
-type f -exec stat -c "%a %n" {} \;

600 /etc/audit/rules.d/audit.rules
640 /etc/audit/audit.rules
640 /etc/audit/auditd.conf
```

Remediation:

Configure the files in directory "/etc/audit/rules.d/" and the "/etc/audit/auditd.conf" file to have a mode of "0640" with the following commands:

```
$ sudo chmod 0640 /etc/audit/rules.d/audit.rules
$ sudo chmod 0640 /etc/audit/rules.d/[customrulesfile].rules
$ sudo chmod 0640 /etc/audit/auditd.conf
```

Additional Information:

CCI-000171 Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system.

- NIST SP 800-53 :: AU-12 b
- NIST SP 800-53 Revision 4 :: AU-12 b
- NIST SP 800-53 Revision 5 :: AU-12 b
- NIST SP 800-53A :: AU-12.1 (iii)

1.388 RHEL-09-653115 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 /etc/audit/auditd.conf file must have 0640 or less permissive to prevent unauthorized access.

```
GROUP ID: V-258172
RULE ID: SV-258172r958444
```

Rationale:

Without the capability to restrict the roles and individuals that can select which events are audited, unauthorized personnel may be able to prevent the auditing of critical events. Misconfigured audits may degrade the system's performance by overwhelming the audit log. Misconfigured audits may also make it more difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit:

Verify the mode of /etc/audit/auditd.conf with the command:

```
$ sudo stat -c "%a %n" /etc/audit/auditd.conf

640 /etc/audit/auditd.conf
```

If "/etc/audit/auditd.conf" does not have a mode of "0640", this is a finding.

Remediation:

Set the mode of /etc/audit/auditd.conf file to 0640 with the command:

```
$ sudo chmod 0640 /etc/audit/auditd.conf
```

Additional Information:

CCI-000171 Allow organization-defined personnel or roles to select the event types that are to be logged by specific components of the system.

- NIST SP 800-53 :: AU-12 b
- NIST SP 800-53 Revision 4 :: AU-12 b
- NIST SP 800-53 Revision 5 :: AU-12 b
- NIST SP 800-53A :: AU-12.1 (iii)

1.389 RHEL-09-653120 (Automated)

Profile Applicability:

- SEVERITY: CAT III

Description:

RHEL 9 must allocate an audit_backlog_limit of sufficient size to capture processes that start prior to the audit daemon.

```
GROUP ID: V-258173
RULE ID: SV-258173r991555
```

Rationale:

Without the capability to generate audit records, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

If auditing is enabled late in the startup process, the actions of some startup processes may not be audited. Some audit systems also maintain state information only available if auditing is enabled before a given process is created.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Allocating an audit_backlog_limit of sufficient size is critical in maintaining a stable boot process. With an insufficient limit allocated, the system is susceptible to boot failures and crashes.

Satisfies: SRG-OS-000254-GPOS-00095, SRG-OS-000341-GPOS-00132

Audit:

Verify RHEL 9 allocates a sufficient audit_backlog_limit to capture processes that start prior to the audit daemon with the following command:

```
$ sudo grubby --info=ALL | grep args | grep -v 'audit_backlog_limit=8192'
```

If the command returns any outputs, and audit_backlog_limit is less than "8192", this is a finding.

Remediation:

Configure RHEL 9 to allocate sufficient audit_backlog_limit to capture processes that start prior to the audit daemon with the following command:

```
$ sudo grubby --update-kernel=ALL --args=audit_backlog_limit=8192
```

Additional Information:

CCI-001464 Initiates session audits automatically at system start-up.

- NIST SP 800-53 :: AU-14 (1)
- NIST SP 800-53 Revision 4 :: AU-14 (1)
- NIST SP 800-53 Revision 5 :: AU-14 (1)
- NIST SP 800-53A :: AU-14 (1).1

CCI-001849 Allocate audit log storage capacity to accommodate organization-defined audit record retention requirements.

- NIST SP 800-53 Revision 4 :: AU-4
- NIST SP 800-53 Revision 5 :: AU-4

1.390 RHEL-09-653125 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must have mail aliases to notify the information system security officer (ISSO) and system administrator (SA) (at a minimum) in the event of an audit processing failure.

```
GROUP ID: V-258174
RULE ID: SV-258174r958424
```

Rationale:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Audit:

Verify that RHEL 9 is configured to notify the appropriate interactive users in the event of an audit processing failure.
Find the alias maps that are being used with the following command:

```
$ postconf alias_maps

alias_maps = hash:/etc/aliases
```

Query the Postfix alias maps for an alias for the root user with the following command:

```
$ postmap -q root hash:/etc/aliases
isso
```

If an alias is not set, this is a finding.

Remediation:

Edit the aliases map file (by default /etc/aliases) used by Postfix and configure a root alias (using the user ISSO as an example):

```
root:    ISSO
```

and then update the aliases database with the command:

```
$ sudo newaliases
```

Additional Information:

CCI-000139 Alert organization-defined personnel or roles within an organization-defined time period in the event of an audit logging process failure.

- NIST SP 800-53 :: AU-5 a
- NIST SP 800-53 Revision 4 :: AU-5 a
- NIST SP 800-53 Revision 5 :: AU-5 a
- NIST SP 800-53A :: AU-5.1 (ii)

1.391 RHEL-09-653130 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 audispd-plugins package must be installed.

```
GROUP ID: V-258175
RULE ID: SV-258175r1045310
```

Rationale:

"audispd-plugins" provides plugins for the real-time interface to the audit subsystem, "audispd". These plugins can do things like relay events to remote machines or analyze events for suspicious behavior.

Audit:

Verify that RHEL 9 has the audispd-plugins package installed with the following command:

```
$ dnf list --installed audispd-plugins
```

Example output:

```
audispd-plugins.x86_64          3.0.7-101.el9_0.2
```

If the "audispd-plugins" package is not installed, this is a finding.

Remediation:

The audispd-plugins package can be installed with the following command:

```
$ sudo dnf install audispd-plugins
```

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4 :: AU-4 (1)
- NIST SP 800-53 Revision 5 :: AU-4 (1)

1.392 RHEL-09-654010 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit uses of the "execve" system call.

```
GROUP ID: V-258176
RULE ID: SV-258176r1045313
```

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.

Satisfies: SRG-OS-000326-GPOS-00126, SRG-OS-000327-GPOS-00127

Audit:

Verify that RHEL 9 is configured to audit the execution of the "execve" system call with the following command:

```
$ sudo auditctl -l | grep execve

-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -F key=execpriv
-a always,exit -F arch=b64 -S execve -C uid!=euid -F euid=0 -F key=execpriv
-a always,exit -F arch=b32 -S execve -C gid!=egid -F egid=0 -F key=execpriv
-a always,exit -F arch=b64 -S execve -C gid!=egid -F egid=0 -F key=execpriv
```

If the command does not return all lines, or the lines are commented out, this is a finding.

Remediation:

Configure RHEL 9 to audit the execution of the "execve" system call.
Add or update the following file system rules to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -k execpriv
-a always,exit -F arch=b64 -S execve -C uid!=euid -F euid=0 -k execpriv
-a always,exit -F arch=b32 -S execve -C gid!=egid -F egid=0 -k execpriv
-a always,exit -F arch=b64 -S execve -C gid!=egid -F egid=0 -k execpriv
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-002233 Prevent the organization-defined software from executing at higher privilege levels than users executing the software.

- NIST SP 800-53 Revision 4 :: AC-6 (8)
- NIST SP 800-53 Revision 5 :: AC-6 (8)

CCI-002234 Log the execution of privileged functions.

- NIST SP 800-53 Revision 4 :: AC-6 (9)
- NIST SP 800-53 Revision 5 :: AC-6 (9)

1.393 RHEL-09-654015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the chmod, fchmod, and fchmodat system calls.

```
GROUP ID: V-258177
RULE ID: SV-258177r1045316
```

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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000064-GPOS-00033, SRG-OS-000466-GPOS-00210, SRG-OS-000458-GPOS-00203

Audit:

Verify that RHEL 9 is configured to audit the execution of the "chmod", "fchmod", and "fchmodat" system calls with the following command:

```
$ sudo auditctl -l | grep chmod

-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 chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1
-F key=perm_mod
```

If both the "b32" and "b64" audit rules are not defined for the "chmod", "fchmod", and "fchmodat" system calls, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "chmod", "fchmod", and "fchmodat" syscalls.
Add or update the following rules in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F
auid!=unset -k perm_mod
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F
auid!=unset -k perm_mod
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.394 RHEL-09-654020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the chown, fchown, fchownat, and lchown system calls.

```
GROUP ID: V-258178
RULE ID: SV-258178r1045319
```

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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000064-GPOS-00033, SRG-OS-000466-GPOS-00210, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Audit:

Verify that RHEL 9 is configured to audit the execution of the "chown", "fchown", "fchownat", and "lchown" system calls with the following command:

```
$ sudo auditctl -l | grep chown

-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 chown,fchown,lchown,fchownat -F auid>=1000 -F
auid!=-1 -F key=perm_mod
```

If both the "b32" and "b64" audit rules are not defined for the "chown", "fchown", "fchownat", and "lchown" system calls, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "chown", "fchown", "fchownat", and "lchown"" system calls.
Add or update the following rules in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S chown,fchown,fchownat,lchown -F auid>=1000 -F
auid!=unset -k perm_mod
-a always,exit -F arch=b64 -S chown,fchown,fchownat,lchown -F auid>=1000 -F
auid!=unset -k perm_mod
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.395 RHEL-09-654025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the setxattr, fsetxattr, lsetxattr, removexattr, fremovexattr, and lremovexattr system calls.

```
GROUP ID: V-258179
RULE ID: SV-258179r1069366
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000462-GPOS-00206, SRG-OS-000463-GPOS-00207, SRG-OS-000471-GPOS-00215, SRG-OS-000474-GPOS-00219, SRG-OS-000466-GPOS-00210, SRG-OS-000064-GPOS-00033

Audit:

Verify RHEL 9 is configured to audit the execution of the "setxattr", "fsetxattr", "lsetxattr", "removexattr", "fremovexattr", and "lremovexattr" system calls with the following command:

```
$ sudo auditctl -l | grep xattr

-a always,exit -F arch=b32 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -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=0
-F key=perm_mod
-a always,exit -F arch=b64 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F auid=0
-F key=perm_mod
```

If both the "b32" and "b64" audit rules are not defined for the "setxattr", "fsetxattr", "lsetxattr", "removexattr", "fremovexattr", and "lremovexattr" system calls, or any of the lines returned are commented out, this is a finding.

Remediation:

Configure RHEL 9 to audit the execution of the "setxattr", "fsetxattr", "lsetxattr", "removexattr", "fremovexattr", and "lremovexattr" system calls by adding or updating the following lines to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F
auid>=1000 -F auid!=unset -k perm_mod
-a always,exit -F arch=b64 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F
auid>=1000 -F auid!=unset -k perm_mod
-a always,exit -F arch=b32 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F auid=0
-k perm_mod
-a always,exit -F arch=b64 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F auid=0
-k perm_mod
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.396 RHEL-09-654030 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of umount system calls.

```
GROUP ID: V-258180
RULE ID: SV-258180r1045325
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that RHEL 9 is configured to audit the execution of the "umount" command with the following command:

```
$ sudo auditctl -l | grep /usr/bin/umount

-a always,exit -S all -F path=/usr/bin/umount -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-mount
```

If the command does not return an audit rule for "umount" or any of the lines returned are commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "umount" command by adding or updating the following rules in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/umount -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-mount
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.397 RHEL-09-654035 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the chacl command.

```
GROUP ID: V-258181
RULE ID: SV-258181r1045328
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000466-GPOS-00210

Audit:

Verify that RHEL 9 is configured to audit the execution of the "chacl" command with the following command:

```
$ sudo auditctl -l | grep chacl

-a always,exit -S all -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F
auid!=-1 -F key=perm_mod
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "chacl" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F auid!=unset
-k perm_mod
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.398 RHEL-09-654040 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the setfacl command.

```
GROUP ID: V-258182
RULE ID: SV-258182r1045331
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that RHEL 9 is configured to audit the execution of the "setfacl" command with the following command:

```
$ sudo auditctl -l | grep setfacl

-a always,exit -S all -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F
auid!=-1 -F key=perm_mod
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "setfacl" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F
auid!=unset -k perm_mod
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.399 RHEL-09-654045 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the chcon command.

```
GROUP ID: V-258183
RULE ID: SV-258183r1045334
```

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).

When a user logs on, the auid is set to the uid of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000468-GPOS-00212, SRG-OS-000471-GPOS-00215, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Audit:

Verify that RHEL 9 is configured to audit the execution of the "chcon" command with the following command:

```
$ sudo auditctl -l | grep chcon

-a always,exit -S all -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F
auid!=-1 -F key=perm_mod
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "chcon" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F auid!=unset
-k perm_mod
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.400 RHEL-09-654050 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the semanage command.

```
GROUP ID: V-258184
RULE ID: SV-258184r1045337
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Audit:

Verify that RHEL 9 is configured to audit the execution of the "semanage" command with the following command:

```
$ sudo auditctl -l | grep semanage

-a always,exit -S all -F path=/usr/sbin/semanage -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "semanage" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/semanage -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)
-

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.401 RHEL-09-654055 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the setfiles command.

```
GROUP ID: V-258185
RULE ID: SV-258185r1045340
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Audit:

Verify that RHEL 9 is configured to audit the execution of the "setfiles" command with the following command:

```
$ sudo auditctl -l | grep setfiles

-a always,exit -S all -F path=/usr/sbin/setfiles -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "setfiles" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/setfiles -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1
-

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.402 RHEL-09-654060 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the setsebool command.

```
GROUP ID: V-258186
RULE ID: SV-258186r1045343
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Audit:

Verify that RHEL 9 is configured to audit the execution of the "setsebool" command with the following command:

```
$ sudo auditctl -l | grep setsebool

-a always,exit -S all -F path=/usr/sbin/setsebool -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate an audit event for any successful/unsuccessful use of the "setsebool " command by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/setsebool -F perm=x -F auid>=1000 -F
auid!=unset -F key=privileged
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.403 RHEL-09-654065 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the rename, unlink, rmdir, renameat, and unlinkat system calls.

```
GROUP ID: V-258187
RULE ID: SV-258187r1045346
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000466-GPOS-00210, SRG-OS-000467-GPOS-00211, SRG-OS-000468-GPOS-00212

Audit:

Verify that RHEL 9 is configured to audit successful/unsuccessful attempts to use the "rename", "unlink", "rmdir", "renameat", and "unlinkat" system calls with the following command:

```
$ sudo auditctl -l | grep 'rename\|unlink\|rmdir'

-a always,exit -F arch=b32 -S unlink,rename,rmdir,unlinkat,renameat -F
auid>=1000 -F auid!=-1 -F key=delete
-a always,exit -F arch=b64 -S rename,rmdir,unlink,unlinkat,renameat -F
auid>=1000 -F auid!=-1 -F key=delete
```

If the command does not return an audit rule for "rename", "unlink", "rmdir", "renameat", and "unlinkat" or any of the lines returned are commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate an audit event for any successful/unsuccessful use of the "rename", "unlink", "rmdir", "renameat", and "unlinkat" system calls by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S rename,unlink,rmdir,renameat,unlinkat -F
auid>=1000 -F auid!=unset -k delete
-a always,exit -F arch=b64 -S rename,unlink,rmdir,renameat,unlinkat -F
auid>=1000 -F auid!=unset -k delete
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.404 RHEL-09-654070 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the truncate, ftruncate, creat, open, openat, and open_by_handle_at system calls.

```
GROUP ID: V-258188
RULE ID: SV-258188r1045349
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205

Audit:

Verify that RHEL 9 is configured to audit successful/unsuccessful attempts to use the "truncate", "ftruncate", "creat", "open", "openat", and "open_by_handle_at" system calls with the following command:

```
$ sudo auditctl -l | grep
'open\b\|openat\|open_by_handle_at\|truncate\|creat'

-a always,exit -F arch=b32 -S
open,creat,truncate,ftruncate,openat,open_by_handle_at -F exit=-EPERM -F
auid>=1000 -F auid!=-1 -F key=perm_access
-a always,exit -F arch=b64 -S
open,truncate,ftruncate,creat,openat,open_by_handle_at -F exit=-EPERM -F
auid>=1000 -F auid!=-1 -F key=perm_access
-a always,exit -F arch=b32 -S
open,creat,truncate,ftruncate,openat,open_by_handle_at -F exit=-EACCES -F
auid>=1000 -F auid!=-1 -F key=perm_access
-a always,exit -F arch=b64 -S
open,truncate,ftruncate,creat,openat,open_by_handle_at -F exit=-EACCES -F
auid>=1000 -F auid!=-1 -F key=perm_access
```

If the output does not produce rules containing "-F exit=-EPERM", this is a finding.
If the output does not produce rules containing "-F exit=-EACCES", this is a finding.
If the command does not return an audit rule for "truncate", "ftruncate", "creat", "open", "openat", and "open_by_handle_at" or any of the lines returned are commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate an audit event for any successful/unsuccessful use of the "truncate", "ftruncate", "creat", "open", "openat", and "open_by_handle_at" system calls by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S
truncate,ftruncate,creat,open,openat,open_by_handle_at -F exit=-EPERM -F
auid>=1000 -F auid!=unset -k perm_access
-a always,exit -F arch=b64 -S
truncate,ftruncate,creat,open,openat,open_by_handle_at -F exit=-EPERM -F
auid>=1000 -F auid!=unset -k perm_access

-a always,exit -F arch=b32 -S
truncate,ftruncate,creat,open,openat,open_by_handle_at -F exit=-EACCES -F
auid>=1000 -F auid!=unset -k perm_access
-a always,exit -F arch=b64 -S
truncate,ftruncate,creat,open,openat,open_by_handle_at -F exit=-EACCES -F
auid>=1000 -F auid!=unset -k perm_access
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.405 RHEL-09-654075 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the delete_module system call.

```
GROUP ID: V-258189
RULE ID: SV-258189r1045352
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Audit:

Verify that RHEL 9 is configured to audit the execution of the "delete_module" system call with the following command:

```
$ sudo auditctl -l | grep delete_module

-a always,exit -F arch=b32 -S delete_module -F auid>=1000 -F auid!=-1 -F
key=module_chng
-a always,exit -F arch=b64 -S delete_module -F auid>=1000 -F auid!=-1 -F
key=module_chng
```

If both the "b32" and "b64" audit rules are not defined for the "delete_module" system call, or any of the lines returned are commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate an audit event for any successful/unsuccessful use of the "delete_module" system call by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S delete_module -F auid>=1000 -F auid!=unset -k
module_chng
-a always,exit -F arch=b64 -S delete_module -F auid>=1000 -F auid!=unset -k
module_chng
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)
-

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.406 RHEL-09-654080 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the init_module and finit_module system calls.

```
GROUP ID: V-258190
RULE ID: SV-258190r1045355
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Audit:

Verify that RHEL 9 is configured to audit the execution of the "init_module" and "finit_module" system calls with the following command:

```
$ sudo auditctl -l | grep init_module

-a always,exit -F arch=b32 -S init_module,finit_module -F auid>=1000 -F
auid!=-1 -F key=module_chng
-a always,exit -F arch=b64 -S init_module,finit_module -F auid>=1000 -F
auid!=-1 -F key=module_chng
```

If both the "b32" and "b64" audit rules are not defined for the "init_module" system call, or any of the lines returned are commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate an audit event for any successful/unsuccessful use of the "init_module" and "finit_module" system calls by adding or updating the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F arch=b32 -S init_module,finit_module -F auid>=1000 -F
auid!=unset -k module_chng
-a always,exit -F arch=b64 -S init_module,finit_module -F auid>=1000 -F
auid!=unset -k module_chng
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)
-

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.407 RHEL-09-654085 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the chage command.

```
GROUP ID: V-258191
RULE ID: SV-258191r1045358
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000468-GPOS-00212, SRG-OS-000471-GPOS-00215

Audit:

Verify that RHEL 9 is configured to audit the execution of the "chage" command with the following command:

```
$ sudo auditctl -l | grep chage

-a always,exit -S all -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-chage
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "chage" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-chage
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.408 RHEL-09-654090 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the chsh command.

```
GROUP ID: V-258192
RULE ID: SV-258192r1045361
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that RHEL 9 is configured to audit the execution of the "chsh" command with the following command:

```
$ sudo auditctl -l | grep chsh

-a always,exit -S all -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F
auid!=-1 -F key=priv_cmd
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "chsh" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F auid!=unset -
k priv_cmd
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.409 RHEL-09-654095 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the crontab command.

```
GROUP ID: V-258193
RULE ID: SV-258193r1045364
```

Rationale:

Audit:

Verify that RHEL 9 is configured to audit the execution of the "crontab" command with the following command:

```
$ sudo auditctl -l | grep crontab

-a always,exit -S all -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-crontab
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "crontab" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-crontab
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)
-

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)
-

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.410 RHEL-09-654100 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the gpasswd command.

```
GROUP ID: V-258194
RULE ID: SV-258194r1045367
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that RHEL 9 is configured to audit the execution of the "gpasswd" command with the following command:

```
$ sudo auditctl -l | grep gpasswd

-a always,exit -S all -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-gpasswd
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "gpasswd" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-gpasswd
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.411 RHEL-09-654105 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the kmod command.

```
GROUP ID: V-258195
RULE ID: SV-258195r1045370
```

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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Audit:

Verify that RHEL 9 is configured to audit the execution of the "kmod" command with the following command:

```
$ sudo auditctl -l | grep kmod

-a always,exit -S all -F path=/usr/bin/kmod -F perm=x -F auid>=1000 -F
auid!=-1 -F key=modules
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "kmod" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/kmod -F perm=x -F auid>=1000 -F auid!=unset -
k modules
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.412 RHEL-09-654110 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the newgrp command.

```
GROUP ID: V-258196
RULE ID: SV-258196r1045373
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that RHEL 9 is configured to audit the execution of the "newgrp" command with the following command:

```
$ sudo auditctl -l | grep newgrp

-a always,exit -S all -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F
auid!=-1 -F key=priv_cmd
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "newgrp" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F auid!=unset
-k priv_cmd
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.413 RHEL-09-654115 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the pam_timestamp_check command.

```
GROUP ID: V-258197
RULE ID: SV-258197r1045376
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that RHEL 9 is configured to audit the execution of the "pam_timestamp_check" command with the following command:

```
$ sudo auditctl -l | grep timestamp

-a always,exit -S all -F path=/usr/sbin/pam_timestamp_check -F perm=x -F
auid>=1000 -F auid!=-1 -F key=privileged-pam_timestamp_check
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "pam_timestamp_check" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/pam_timestamp_check -F perm=x -F auid>=1000
-F auid!=unset -k privileged-pam_timestamp_check
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.414 RHEL-09-654120 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the passwd command.

```
GROUP ID: V-258198
RULE ID: SV-258198r1045379
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify RHEL 9 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/gshadow" with the following command:

```
$ sudo auditctl -l | egrep '(/usr/bin/passwd)'

-a always,exit -S all -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-passwd
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "passwd" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-passwd
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.415 RHEL-09-654125 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the postdrop command.

```
GROUP ID: V-258199
RULE ID: SV-258199r1045382
```

Rationale:

Without generating audit records 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that RHEL 9 is configured to audit the execution of the "postdrop" command with the following command:

```
$ sudo auditctl -l | grep postdrop

-a always,exit -S all -F path=/usr/sbin/postdrop -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "postdrop" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/postdrop -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the

- audit records.
- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.416 RHEL-09-654130 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the postqueue command.

```
GROUP ID: V-258200
RULE ID: SV-258200r1045385
```

Rationale:

Without generating audit record 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that RHEL 9 is configured to audit the execution of the "postqueue" command with the following command:

```
$ sudo auditctl -l | grep postqueue

-a always,exit -S all -F path=/usr/sbin/postqueue -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "postqueue" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/postqueue -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.417 RHEL-09-654135 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the ssh-agent command.

```
GROUP ID: V-258201
RULE ID: SV-258201r1045388
```

Rationale:

Without generating audit record 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that RHEL 9 is configured to audit the execution of the "ssh-agent" command with the following command:

```
$ sudo auditctl -l | grep ssh-agent

-a always,exit -S all -F path=/usr/bin/ssh-agent -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-ssh
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "ssh-agent" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/ssh-agent -F perm=x -F auid>=1000 -F auid!=unset -k privileged-ssh
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.418 RHEL-09-654140 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the ssh-keysign command.

```
GROUP ID: V-258202
RULE ID: SV-258202r1045391
```

Rationale:

Without generating audit record 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that RHEL 9 is configured to audit the execution of the "ssh-keysign" command with the following command:

```
$ sudo auditctl -l | grep ssh-keysign

-a always,exit -S all -F path=/usr/libexec/openssh/ssh-keysign -F perm=x -F
auid>=1000 -F auid!=-1 -F key=privileged-ssh
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "ssh-keysign" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/libexec/openssh/ssh-keysign -F perm=x -F
auid>=1000 -F auid!=unset -k privileged-ssh
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.419 RHEL-09-654145 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the su command.

```
GROUP ID: V-258203
RULE ID: SV-258203r1045394
```

Rationale:

Without generating audit record 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000466-GPOS-00210

Audit:

Verify that RHEL 9 is configured to audit the execution of the "su" command with the following command:

```
$ sudo auditctl -l | grep '/usr/bin/su\b'

-a always,exit -S all -F path=/usr/bin/su -F perm=x -F auid>=1000 -F auid!=-1
-F key=privileged-priv_change
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "su" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/su -F perm=x -F auid>=1000 -F auid!=unset -k privileged-priv_change
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.420 RHEL-09-654150 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the sudo command.

```
GROUP ID: V-258204
RULE ID: SV-258204r1045397
```

Rationale:

Without generating audit record 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000466-GPOS-00210

Audit:

Verify that RHEL 9 is configured to audit the execution of the "sudo" command with the following command:

```
$ sudo auditctl -l | grep '/usr/bin/sudo\b'

-a always,exit -S all -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F
auid!=-1 -F key=priv_cmd
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "sudo" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F auid!=unset -
k priv_cmd
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.421 RHEL-09-654155 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the sudoedit command.

```
GROUP ID: V-258205
RULE ID: SV-258205r1045400
```

Rationale:

Without generating audit record 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that RHEL 9 is configured to audit the execution of the "sudoedit" command with the following command:

```
$ sudo auditctl -l | grep /usr/bin/sudoedit

-a always,exit -S all -F path=/usr/bin/sudoedit -F perm=x -F auid>=1000 -F
auid!=-1 -F key=priv_cmd
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "sudoedit" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/sudoedit -F perm=x -F auid>=1000 -F
auid!=unset -k priv_cmd
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.422 RHEL-09-654160 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the unix_chkpwd command.

```
GROUP ID: V-258206
RULE ID: SV-258206r1045403
```

Rationale:

Without generating audit record 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that RHEL 9 is configured to audit the execution of the "unix_chkpwd" command with the following command:

```
$ sudo auditctl -l | grep unix_chkpwd

-a always,exit -S all -F path=/usr/sbin/unix_chkpwd -F perm=x -F auid>=1000 -
F auid!=-1 -F key=privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "unix_chkpwd" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/unix_chkpwd -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.423 RHEL-09-654165 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the unix_update command.

```
GROUP ID: V-258207
RULE ID: SV-258207r1045406
```

Rationale:

Without generating audit record 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that RHEL 9 is configured to audit the execution of the "unix_update" command with the following command:

```
$ sudo auditctl -l | grep unix_update

-a always,exit -S all -F path=/usr/sbin/unix_update -F perm=x -F auid>=1000 -
F auid!=-1 -F key=privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "unix_update" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/unix_update -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.424 RHEL-09-654170 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the userhelper command.

```
GROUP ID: V-258208
RULE ID: SV-258208r1045409
```

Rationale:

Without generating audit record 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that RHEL 9 is configured to audit the execution of the "userhelper" command with the following command:

```
$ sudo auditctl -l | grep userhelper

-a always,exit -S all -F path=/usr/sbin/userhelper -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-unix-update
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "userhelper" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/userhelper -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-unix-update
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.425 RHEL-09-654175 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the usermod command.

```
GROUP ID: V-258209
RULE ID: SV-258209r1045412
```

Rationale:

Without generating audit record 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).

When a user logs on, the auid is set to the uid of the account being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000466-GPOS-00210

Audit:

Verify that RHEL 9 is configured to audit the execution of the "usermod" command with the following command:

```
$ sudo auditctl -l | grep usermod

-a always,exit -S all -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-usermod
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "usermod " command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-usermod
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.426 RHEL-09-654180 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must audit all uses of the mount command.

```
GROUP ID: V-258210
RULE ID: SV-258210r1045415
```

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).

When a user logs on, the auid is set to the uid of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

The system call rules are loaded into a matching engine that intercepts each system call made by all programs on the system. Therefore, it is very important to use system call rules only when absolutely necessary since these affect performance. The more rules, the bigger the performance hit. The performance can be helped, however, by combining system calls into one rule whenever possible.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that RHEL 9 is configured to audit the execution of the "mount" command with the following command:

```
$ sudo auditctl -l | grep /usr/bin/mount

-a always,exit -S all -F path=/usr/bin/mount -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-mount
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records upon successful/unsuccessful attempts to use the "mount" command by adding or updating the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/mount -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-mount
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.427 RHEL-09-654185 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Successful/unsuccessful uses of the init command in RHEL 9 must generate an audit record.

```
GROUP ID: V-258211
RULE ID: SV-258211r1045418
```

Rationale:

Misuse of the init command may cause availability issues for the system.

Audit:

Verify that RHEL 9 is configured to audit the execution of the "init" command with the following command:

```
$ sudo auditctl -l | grep /usr/sbin/init

-a always,exit -S all -F path=/usr/sbin/init -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-init
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "init" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/init -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-init
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

1.428 RHEL-09-654190 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Successful/unsuccessful uses of the poweroff command in RHEL 9 must generate an audit record.

```
GROUP ID: V-258212
RULE ID: SV-258212r1045421
```

Rationale:

Misuse of the poweroff command may cause availability issues for the system.

Audit:

Verify that RHEL 9 is configured to audit the execution of the "poweroff" command with the following command:

```
$ sudo auditctl -l | grep poweroff

-a always,exit -S all -F path=/usr/sbin/poweroff -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-poweroff
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "poweroff" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/poweroff -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-poweroff
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

1.429 RHEL-09-654195 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Successful/unsuccessful uses of the reboot command in RHEL 9 must generate an audit record.

```
GROUP ID: V-258213
RULE ID: SV-258213r1045424
```

Rationale:

Misuse of the reboot command may cause availability issues for the system.

Audit:

Verify that RHEL 9 is configured to audit the execution of the "reboot" command with the following command:

```
$ sudo auditctl -l | grep reboot

-a always,exit -S all -F path=/usr/sbin/reboot -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-reboot
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "reboot" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/reboot -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-reboot
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

1.430 RHEL-09-654200 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Successful/unsuccessful uses of the shutdown command in RHEL 9 must generate an audit record.

```
GROUP ID: V-258214
RULE ID: SV-258214r1045427
```

Rationale:

Misuse of the shutdown command may cause availability issues for the system.

Audit:

Verify that RHEL 9 is configured to audit the execution of the "shutdown" command with the following command:

```
$ sudo cat /etc/audit/rules.d/* | grep shutdown

-a always,exit -S all -F path=/usr/sbin/shutdown -F perm=x -F auid>=1000 -F
auid!=-1 -F key=privileged-shutdown
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful uses of the "shutdown" command by adding or updating the following rule in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/shutdown -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-shutdown
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

1.431 RHEL-09-654205 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Successful/unsuccessful uses of the umount system call in RHEL 9 must generate an audit record.

```
GROUP ID: V-258215
RULE ID: SV-258215r1045430
```

Rationale:

The changing of file permissions could indicate that a user is attempting to gain access to information that would otherwise be disallowed. Auditing DAC modifications can facilitate the identification of patterns of abuse among both authorized and unauthorized users.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify that RHEL 9 generates an audit record for all uses of the "umount" and system call with the following command:

```
$ sudo auditctl -l | grep b32 | grep 'umount\b'

-a always,exit -F arch=b32 -S umount -F auid>=1000 -F auid!=-1 -F
key=privileged-umount
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "umount" system call by adding or updating the following rules in "/etc/audit/audit.rules" and adding the following rules to "/etc/audit/rules.d/perm_mod.rules" or updating the existing rules in files in the "/etc/audit/rules.d/" directory:

```
-a always,exit -F arch=b32 -S umount -F auid>=1000 -F auid!=unset -k
privileged-umount
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.432 RHEL-09-654210 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

Successful/unsuccessful uses of the umount2 system call in RHEL 9 must generate an audit record.

```
GROUP ID: V-258216
RULE ID: SV-258216r1045433
```

Rationale:

The changing of file permissions could indicate that a user is attempting to gain access to information that would otherwise be disallowed. Auditing DAC modifications can facilitate the identification of patterns of abuse among both authorized and unauthorized users.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

To determine if the system is configured to audit calls to the umount2 system call, run the following command:

```
$ sudo auditctl -l | grep umount2

-a always,exit -F arch=b64 -S umount2 -F auid>=1000 -F auid!=-1 -F
key=privileged-umount
-a always,exit -F arch=b32 -S umount2 -F auid>=1000 -F auid!=-1 -F
key=privileged-umount
```

If no line is returned, this is a finding.

Remediation:

Configure the audit system to generate an audit event for any successful/unsuccessful use of the "umount2" system call by adding or updating the following rules in a file in "/etc/audit/rules.d".

```
-a always,exit -F arch=b32 -S umount2 -F auid>=1000 -F auid!=unset -k
privileged-umount
-a always,exit -F arch=b64 -S umount2 -F auid>=1000 -F auid!=unset -k
privileged-umount
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.433 RHEL-09-654215 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/sudoers.

```
GROUP ID: V-258217
RULE ID: SV-258217r1045436
```

Rationale:

The actions taken by system administrators must be audited to keep a record of what was executed on the system, as well as for accountability purposes. Editing the sudoers file may be sign of an attacker trying to establish persistent methods to a system, auditing the editing of the sudoers files mitigates this risk.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221

Audit:

Verify RHEL 9 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers" with the following command:

```
$ sudo auditctl -l | grep '/etc/sudoers[^.]'

-w /etc/sudoers -p wa -k identity
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers".
Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/sudoers -p wa -k identity
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001404 Automatically audit account disabling actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001405 Automatically audit account removal actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-002130 Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)

CCI-000015 Support the management of system accounts using (organization-defined automated mechanisms).

- NIST SP 800-53 :: AC-2 (1)
- NIST SP 800-53 Revision 4 :: AC-2 (1)
- NIST SP 800-53 Revision 5 :: AC-2 (1)
- NIST SP 800-53A :: AC-2 (1).1

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)

1.434 RHEL-09-654220 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/sudoers.d/ directory.

```
GROUP ID: V-258218
RULE ID: SV-258218r1045439
```

Rationale:

The actions taken by system administrators must be audited to keep a record of what was executed on the system, as well as for accountability purposes. Editing the sudoers file may be sign of an attacker trying to establish persistent methods to a system, auditing the editing of the sudoers files mitigates this risk.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221

Audit:

Verify RHEL 9 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers.d/" with the following command:

```
$ sudo auditctl -l | grep /etc/sudoers.d

-w /etc/sudoers.d -p wa -k actions
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/sudoers.d/".
Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/sudoers.d/ -p wa -k identity
```

To load the rules to the kernel immediately, use the following command:

```
$ sudo augenrules --load
```

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001404 Automatically audit account disabling actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001405 Automatically audit account removal actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-002130 Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)

CCI-000015 Support the management of system accounts using (organization-defined automated mechanisms).

- NIST SP 800-53 :: AC-2 (1)
- NIST SP 800-53 Revision 4 :: AC-2 (1)
- NIST SP 800-53 Revision 5 :: AC-2 (1)
- NIST SP 800-53A :: AC-2 (1).1

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)

1.435 RHEL-09-654225 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/group.

```
GROUP ID: V-258219
RULE ID: SV-258219r1015130
```

Rationale:

In addition to auditing new user and group accounts, these watches will alert the system administrator(s) to any modifications. Any unexpected users, groups, or modifications must be investigated for legitimacy.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221

Audit:

Verify RHEL 9 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/group" with the following command:

```
$ sudo auditctl -l | egrep '(/etc/group)'

-w /etc/group -p wa -k identity
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/group".
Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/group -p wa -k identity
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001404 Automatically audit account disabling actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001405 Automatically audit account removal actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-002130 Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)

CCI-000015 Support the management of system accounts using (organization-defined automated mechanisms).

- NIST SP 800-53 :: AC-2 (1)
- NIST SP 800-53 Revision 4 :: AC-2 (1)
- NIST SP 800-53 Revision 5 :: AC-2 (1)
- NIST SP 800-53A :: AC-2 (1).1

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)

1.436 RHEL-09-654230 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/gshadow.

```
GROUP ID: V-258220
RULE ID: SV-258220r1015131
```

Rationale:

In addition to auditing new user and group accounts, these watches will alert the system administrator(s) to any modifications. Any unexpected users, groups, or modifications should be investigated for legitimacy.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221

Audit:

Verify RHEL 9 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/gshadow" with the following command:

```
$ sudo auditctl -l | egrep '(/etc/gshadow)'

-w /etc/gshadow -p wa -k identity
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/gshadow".
Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/gshadow -p wa -k identity
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001404 Automatically audit account disabling actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001405 Automatically audit account removal actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-002130 Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)

CCI-000015 Support the management of system accounts using (organization-defined automated mechanisms).

- NIST SP 800-53 :: AC-2 (1)
- NIST SP 800-53 Revision 4 :: AC-2 (1)
- NIST SP 800-53 Revision 5 :: AC-2 (1)
- NIST SP 800-53A :: AC-2 (1).1

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)

1.437 RHEL-09-654235 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/opasswd.

```
GROUP ID: V-258221
RULE ID: SV-258221r1015132
```

Rationale:

In addition to auditing new user and group accounts, these watches will alert the system administrator(s) to any modifications. Any unexpected users, groups, or modifications should be investigated for legitimacy.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221

Audit:

Verify RHEL 9 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/security/opasswd" with the following command:

```
$ sudo auditctl -l | egrep '(/etc/security/opasswd)'

-w /etc/security/opasswd -p wa -k identity
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/security/opasswd".
Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/security/opasswd -p wa -k identity
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001404 Automatically audit account disabling actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001405 Automatically audit account removal actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-002130 Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)

CCI-000015 Support the management of system accounts using (organization-defined automated mechanisms).

- NIST SP 800-53 :: AC-2 (1)
- NIST SP 800-53 Revision 4 :: AC-2 (1)
- NIST SP 800-53 Revision 5 :: AC-2 (1)
- NIST SP 800-53A :: AC-2 (1).1

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)

1.438 RHEL-09-654240 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd.

```
GROUP ID: V-258222
RULE ID: SV-258222r1015133
```

Rationale:

In addition to auditing new user and group accounts, these watches will alert the system administrator(s) to any modifications. Any unexpected users, groups, or modifications should be investigated for legitimacy.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221, SRG-OS-000274-GPOS-00104, SRG-OS-000275-GPOS-00105, SRG-OS-000276-GPOS-00106, SRG-OS-000277-GPOS-00107

Audit:

Verify RHEL 9 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd" with the following command:

```
$ sudo auditctl -l | egrep '(/etc/passwd)'

-w /etc/passwd -p wa -k identity
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd".
Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/passwd -p wa -k identity
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

CCI-000015 Support the management of system accounts using (organization-defined automated mechanisms).

- NIST SP 800-53 :: AC-2 (1)
- NIST SP 800-53 Revision 4 :: AC-2 (1)
- NIST SP 800-53 Revision 5 :: AC-2 (1)
- NIST SP 800-53A :: AC-2 (1).1

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001404 Automatically audit account disabling actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001405 Automatically audit account removal actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-002130 Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

CCI-001683 The information system notifies organization-defined personnel or roles for account creation actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001684 The information system notifies organization-defined personnel or roles for account modification actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001685 The information system notifies organization-defined personnel or roles for account disabling actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001686 The information system notifies organization-defined personnel or roles for account removal actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)

1.439 RHEL-09-654245 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow.

```
GROUP ID: V-258223
RULE ID: SV-258223r1015134
```

Rationale:

In addition to auditing new user and group accounts, these watches will alert the system administrator(s) to any modifications. Any unexpected users, groups, or modifications should be investigated for legitimacy.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000304-GPOS-00121, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000470-GPOS-00214, SRG-OS-000471-GPOS-00215, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000466-GPOS-00210, SRG-OS-000476-GPOS-00221

Audit:

Verify RHEL 9 generates audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd with the following command:

```
$ sudo auditctl -l | egrep '(/etc/shadow)'

-w /etc/shadow -p wa -k identity
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/shadow".
Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/shadow -p wa -k identity
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001404 Automatically audit account disabling actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-001405 Automatically audit account removal actions.

- NIST SP 800-53 :: AC-2 (4)
- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)
- NIST SP 800-53A :: AC-2 (4).1 (i and ii)

CCI-002130 Automatically audit account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)
- NIST SP 800-53 Revision 5 :: AC-2 (4)

CCI-000015 Support the management of system accounts using (organization-defined automated mechanisms).

- NIST SP 800-53 :: AC-2 (1)
- NIST SP 800-53 Revision 4 :: AC-2 (1)
- NIST SP 800-53 Revision 5 :: AC-2 (1)
- NIST SP 800-53A :: AC-2 (1).1

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.

- NIST SP 800-53 Revision 4 :: AC-2 (4)

1.440 RHEL-09-654250 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must generate audit records for all account creations, modifications, disabling, and termination events that affect /var/log/faillock.

```
GROUP ID: V-258224
RULE ID: SV-258224r1014988
```

Rationale:

Without generating audit records 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.

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Audit:

Verify RHEL 9 generates audit records for all account creations, modifications, disabling, and termination events that affect "/var/log/faillock" with the following command:

```
$ sudo auditctl -l | grep /var/log/faillock

-w /var/log/faillock -p wa -k logins
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records for all account creations, modifications, disabling, and termination events that affect "/var/log/faillock".
Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /var/log/faillock -p wa -k logins
```

The audit daemon must be restarted for the changes to take effect.

```
$ sudo service auditd restart
```

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.441 RHEL-09-654255 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must generate audit records for all account creations, modifications, disabling, and termination events that affect /var/log/lastlog.

```
GROUP ID: V-258225
RULE ID: SV-258225r1014990
```

Rationale:

Without generating audit records 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.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000473-GPOS-00218, SRG-OS-000470-GPOS-00214

Audit:

Verify RHEL 9 generates audit records for all account creations, modifications, disabling, and termination events that affect "/var/log/lastlog" with the following command:

```
$ sudo auditctl -l | grep /var/log/lastlog

-w /var/log/lastlog -p wa -k logins
```

If the command does not return a line, or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 to generate audit records for all account creations, modifications, disabling, and termination events that affect "/var/log/lastlog".
Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /var/log/lastlog -p wa -k logins
```

The audit daemon must be restarted for the changes to take effect.

```
$ sudo service auditd restart
```

Additional Information:

CCI-000130 Ensure that audit records containing information that establishes what type of event occurred.

- NIST SP 800-53 :: AU-3
- NIST SP 800-53 Revision 4 :: AU-3
- NIST SP 800-53 Revision 5 :: AU-3 a
- NIST SP 800-53A :: AU-3.1

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

- NIST SP 800-53 :: AU-3 (1)
- NIST SP 800-53 Revision 4 :: AU-3 (1)
- NIST SP 800-53 Revision 5 :: AU-3 (1)
- NIST SP 800-53A :: AU-3 (1).1 (ii)

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a. on organization-defined information system components.

- NIST SP 800-53 :: AU-12 a
- NIST SP 800-53 Revision 4 :: AU-12 a
- NIST SP 800-53 Revision 5 :: AU-12 a
- NIST SP 800-53A :: AU-12.1 (ii)

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.442 RHEL-09-654260 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must generate audit records for all account creations, modifications, disabling, and termination events that affect /var/log/tallylog.

```
GROUP ID: V-258226
RULE ID: SV-258226r958846
```

Rationale:

Without generating audit records 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.

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Audit:

Verify RHEL 9 generates audit records for all account creations, modifications, disabling, and termination events that affect "/var/log/tallylog" with the following command:

```
$ sudo auditctl -l | grep /var/log/tallylog

-w /var/log/tallylog -p wa -k logins
```

If the command does not return a line, or the line is commented out, is a finding.

Remediation:

Configure RHEL 9 to generate audit records for all account creations, modifications, disabling, and termination events that affect "/var/log/tallylog".
Add or update the following file system rule to "/etc/audit/rules.d/audit.rules":

```
-w /var/log/tallylog -p wa -k logins
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

CCI-002884 Log organization-defined audit events for nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 Revision 4 :: MA-4 (1) (a)
- NIST SP 800-53 Revision 5 :: MA-4 (1) (a)

1.443 RHEL-09-654265 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must take appropriate action when a critical audit processing failure occurs.

```
GROUP ID: V-258227
RULE ID: SV-258227r1014992
```

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.

Satisfies: SRG-OS-000046-GPOS-00022, SRG-OS-000047-GPOS-00023

Audit:

Verify the audit service is configured to panic on a critical error with the following command:

```
$ sudo grep "\-f" /etc/audit/audit.rules

-f 2
```

If the value for "-f" is not "2", and availability is not documented as an overriding concern, this is a finding.

Remediation:

Configure RHEL 9 to shut down when auditing failures occur.
Add the following line to the bottom of the /etc/audit/rules.d/audit.rules file:

```
-f 2
```

Additional Information:

CCI-000139 Alert organization-defined personnel or roles within an organization-defined time period in the event of an audit logging process failure.

- NIST SP 800-53 :: AU-5 a
- NIST SP 800-53 Revision 4 :: AU-5 a
- NIST SP 800-53 Revision 5 :: AU-5 a
- NIST SP 800-53A :: AU-5.1 (ii)

CCI-000140 Take organization-defined actions upon audit failure include, shutting down the system, overwriting oldest audit records, and stopping the generation of audit records.

- NIST SP 800-53 :: AU-5 b
- NIST SP 800-53 Revision 4 :: AU-5 b
- NIST SP 800-53 Revision 5 :: AU-5 b
- NIST SP 800-53A :: AU-5.1 (iv)

1.444 RHEL-09-654270 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 audit system must protect logon UIDs from unauthorized change.

```
GROUP ID: V-258228
RULE ID: SV-258228r991572
```

Rationale:

If modification of login user identifiers (UIDs) is not prevented, they can be changed by nonprivileged users and make auditing complicated or impossible.

Satisfies: SRG-OS-000462-GPOS-00206, SRG-OS-000475-GPOS-00220, SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify the audit system prevents unauthorized changes to logon UIDs with the following command:

```
$ sudo grep -i immutable /etc/audit/audit.rules

--loginuid-immutable
```

If the "--loginuid-immutable" option is not returned in the "/etc/audit/audit.rules", or the line is commented out, this is a finding.

Remediation:

Configure RHEL 9 auditing to prevent modification of login UIDs once they are set by adding the following line to /etc/audit/rules.d/audit.rules:

```
--loginuid-immutable
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53 :: AU-12 c
- NIST SP 800-53 Revision 4 :: AU-12 c
- NIST SP 800-53 Revision 5 :: AU-12 c
- NIST SP 800-53A :: AU-12.1 (iv)

1.445 RHEL-09-654275 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 audit system must protect auditing rules from unauthorized change.

```
GROUP ID: V-258229
RULE ID: SV-258229r958434
```

Rationale:

Unauthorized disclosure of audit records can reveal system and configuration data to attackers, thus compromising its confidentiality.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit RHEL 9 system activity.

In immutable mode, unauthorized users cannot execute changes to the audit system to potentially hide malicious activity and then put the audit rules back. A system reboot would be noticeable, and a system administrator could then investigate the unauthorized changes.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify the audit system prevents unauthorized changes with the following command:

```
$ sudo grep "^\s*[^#]" /etc/audit/audit.rules | tail -1

-e 2
```

If the audit system is not set to be immutable by adding the "-e 2" option to the end of "/etc/audit/audit.rules", this is a finding.

Remediation:

Configure the audit system to set the audit rules to be immutable by adding the following line to end of "/etc/audit/rules.d/audit.rules"

```
-e 2
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53 :: AU-9
- NIST SP 800-53 Revision 4 :: AU-9
- NIST SP 800-53 Revision 5 :: AU-9 a
- NIST SP 800-53A :: AU-9.1

1.446 RHEL-09-671010 (Automated)

Profile Applicability:

- SEVERITY: CAT I

Description:

RHEL 9 must enable FIPS mode.

```
GROUP ID: V-258230
RULE ID: SV-258230r958408
```

Rationale:

Use of weak or untested encryption algorithms undermines the purposes of utilizing 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. This includes NIST FIPS-validated cryptography for the following: Provisioning digital signatures, generating cryptographic hashes, and to protect data requiring data-at-rest protections in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000125-GPOS-00065, SRG-OS-000396-GPOS-00176, SRG-OS-000423-GPOS-00187, SRG-OS-000478-GPOS-00223

Audit:

Verify that RHEL 9 is in FIPS mode with the following command:

```
$ sudo fips-mode-setup --check

FIPS mode is enabled.
```

If FIPS mode is not enabled, this is a finding.

Remediation:

Configure the operating system to implement FIPS mode with the following command

```
$ sudo fips-mode-setup --enable
```

Reboot the system for the changes to take effect.

Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53 :: AC-17 (2)
- NIST SP 800-53 Revision 4 :: AC-17 (2)
- NIST SP 800-53 Revision 5 :: AC-17 (2)
- NIST SP 800-53A :: AC-17 (2).1

CCI-000877 Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53 :: MA-4 c
- NIST SP 800-53 Revision 4 :: MA-4 c
- NIST SP 800-53 Revision 5 :: MA-4 c
- NIST SP 800-53A :: MA-4.1 (iv)

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4 :: SC-8
- NIST SP 800-53 Revision 5 :: SC-8

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4 :: SC-13
- NIST SP 800-53 Revision 5 :: SC-13 b

1.447 RHEL-09-671015 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must employ FIPS 140-3 approved cryptographic hashing algorithms for all stored passwords.

```
GROUP ID: V-258231
RULE ID: SV-258231r1069375
```

Rationale:

The system must use a strong hashing algorithm to store the password.

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.

Satisfies: SRG-OS-000073-GPOS-00041, SRG-OS-000120-GPOS-00061

Audit:

Verify the interactive user account passwords are using a strong password hash with the following command:

```
$ sudo cut -d: -f2 /etc/shadow

$6$kcOnRq/5$NUEYPuyL.wghQwWssXRcLRFiiru7f5JPV6GaJhNC2aK5F3PZpE/BCCtwrxRc/AInK
MNX3CdMw11m9STiql12f/
```

Password hashes "!" or "*" indicate inactive accounts not available for logon and are not evaluated.
If any interactive user password hash does not begin with "6", this is a finding.

Remediation:

Lock all interactive user accounts not using SHA-512 hashing until the passwords can be regenerated with SHA-512.

Additional Information:

CCI-004062 For password-based authentication, store passwords using an approved salted key derivation function, preferably using a keyed hash.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (d)

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53 :: IA-7
- NIST SP 800-53 Revision 4 :: IA-7
- NIST SP 800-53 Revision 5 :: IA-7
- NIST SP 800-53A :: IA-7.1

CCI-000196 The information system, for password-based authentication, stores only cryptographically-protected passwords.

- NIST SP 800-53 :: IA-5 (1) (c)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (c)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.448 RHEL-09-671020 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 IP tunnels must use FIPS 140-3 approved cryptographic algorithms.

```
GROUP ID: V-258232
RULE ID: SV-258232r1045440
```

Rationale:

Overriding the system crypto policy makes the behavior of the Libreswan service violate expectations, and makes system configuration more fragmented.

Audit:

Verify that the IPsec service uses the system crypto policy with the following command:
Note: If the ipsec service is not installed, this requirement is Not Applicable.

```
$ sudo grep include /etc/ipsec.conf /etc/ipsec.d/*.conf

/etc/ipsec.conf:include /etc/crypto-policies/back-ends/libreswan.config
```

If the ipsec configuration file does not contain "include /etc/crypto-policies/back-ends/libreswan.config", this is a finding.

Remediation:

Configure Libreswan to use the system cryptographic policy.
Add the following line to "/etc/ipsec.conf":

```
include /etc/crypto-policies/back-ends/libreswan.config
```

Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53 :: AC-17 (2)
- NIST SP 800-53 Revision 4 :: AC-17 (2)
- NIST SP 800-53 Revision 5 :: AC-17 (2)
- NIST SP 800-53A :: AC-17 (2).1

1.449 RHEL-09-671025 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 pam_unix.so module must be configured in the password-auth file to use a FIPS 140-3 approved cryptographic hashing algorithm for system authentication.

```
GROUP ID: V-258233
RULE ID: SV-258233r1015136
```

Rationale:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and; therefore, cannot be relied upon to provide confidentiality or integrity, and DOD data may be compromised.

RHEL 9 systems utilizing encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

FIPS 140-3 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DOD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general-purpose computing system.

Audit:

Verify that the pam_unix.so module is configured to use sha512 in /etc/pam.d/password-auth with the following command:

```
$ grep "^password.*pam_unix.so.*sha512" /etc/pam.d/password-auth

password sufficient pam_unix.so sha512
```

If "sha512" is missing, or the line is commented out, this is a finding.
If the system administrator (SA) can demonstrate that the required configuration is contained in a PAM configuration file included or substacked from the system-auth file, this is not a finding.

Remediation:

Configure RHEL 9 to use a FIPS 140-3 approved cryptographic hashing algorithm for system authentication.
Edit/modify the following line in the "/etc/pam.d/password-auth" file to include the sha512 option for pam_unix.so:

```
password sufficient pam_unix.so sha512
```

Additional Information:

CCI-004062 For password-based authentication, store passwords using an approved salted key derivation function, preferably using a keyed hash.

- NIST SP 800-53 Revision 5 :: IA-5 (1) (d)

CCI-000196 The information system, for password-based authentication, stores only cryptographically-protected passwords.

- NIST SP 800-53 :: IA-5 (1) (c)
- NIST SP 800-53 Revision 4 :: IA-5 (1) (c)
- NIST SP 800-53A :: IA-5 (1).1 (v)

1.450 RHEL-09-672020 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

RHEL 9 cryptographic policy must not be overridden.

GROUP ID: V-258236 RULE ID: SV-258236r1051253

Rationale:

Centralized cryptographic policies simplify applying secure ciphers across an operating system and the applications that run on that operating system. Use of weak or untested encryption algorithms undermines the purposes of using encryption to protect data.

Satisfies: SRG-OS-000396-GPOS-00176, SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174

Audit:

Verify that RHEL 9 cryptographic policies are not overridden.
Verify that the configured policy matches the generated policy with the following command:

```
$ sudo update-crypto-policies --check && echo PASS

The configured policy matches the generated policy
PASS
```

If the last line is not "PASS", this is a finding.
List all of the crypto backends configured on the system with the following command:

```
$ ls -l /etc/crypto-policies/back-ends/

lrwxrwxrwx. 1 root root  40 Nov 13 16:29 bind.config -> /usr/share/crypto-
policies/FIPS/bind.txt
lrwxrwxrwx. 1 root root  42 Nov 13 16:29 gnutls.config -> /usr/share/crypto-
policies/FIPS/gnutls.txt
lrwxrwxrwx. 1 root root  40 Nov 13 16:29 java.config -> /usr/share/crypto-
policies/FIPS/java.txt
lrwxrwxrwx. 1 root root  46 Nov 13 16:29 javasystem.config ->
/usr/share/crypto-policies/FIPS/javasystem.txt
lrwxrwxrwx. 1 root root  40 Nov 13 16:29 krb5.config -> /usr/share/crypto-
policies/FIPS/krb5.txt
lrwxrwxrwx. 1 root root  45 Nov 13 16:29 libreswan.config ->
/usr/share/crypto-policies/FIPS/libreswan.txt
lrwxrwxrwx. 1 root root  42 Nov 13 16:29 libssh.config -> /usr/share/crypto-
policies/FIPS/libssh.txt
-rw-r--r--. 1 root root 398 Nov 13 16:29 nss.config
lrwxrwxrwx. 1 root root  43 Nov 13 16:29 openssh.config -> /usr/share/crypto-
policies/FIPS/openssh.txt
lrwxrwxrwx. 1 root root  49 Nov 13 16:29 opensshserver.config ->
/usr/share/crypto-policies/FIPS/opensshserver.txt
lrwxrwxrwx. 1 root root  46 Nov 13 16:29 opensslcnf.config ->
/usr/share/crypto-policies/FIPS/opensslcnf.txt
lrwxrwxrwx. 1 root root  43 Nov 13 16:29 openssl.config -> /usr/share/crypto-
policies/FIPS/openssl.txt
lrwxrwxrwx. 1 root root  48 Nov 13 16:29 openssl_fips.config ->
/usr/share/crypto-policies/FIPS/openssl_fips.txt
```

If the paths do not point to the respective files under /usr/share/crypto-policies/FIPS path, this is a finding.
Note: nss.config should not be hyperlinked.

Remediation:

Configure RHEL 9 to correctly implement the systemwide cryptographic policies by reinstalling the crypto-policies package contents.
Reinstall crypto-policies with the following command:

```
$ sudo dnf -y reinstall crypto-policies
```

Set the crypto-policy to FIPS with the following command:

```
$ sudo update-crypto-policies --set FIPS

Setting system policy to FIPS
```

Note: Systemwide crypto policies are applied on application startup. It is recommended to restart the system for the change of policies to fully take place.

Additional Information:

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4 :: SC-13
- NIST SP 800-53 Revision 5 :: SC-13 b

CCI-002890 Implement organization-defined cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4 :: MA-4 (6)
- NIST SP 800-53 Revision 5 :: MA-4 (6)

CCI-003123 Implement organization-defined cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4 :: MA-4 (6)
- NIST SP 800-53 Revision 5 :: MA-4 (6)

1.451 RHEL-09-672025 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must use mechanisms meeting the requirements of applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

GROUP ID: V-258237 RULE ID: SV-258237r1051256

Rationale:

Overriding the system crypto policy makes the behavior of Kerberos violate expectations and makes system configuration more fragmented.

Audit:

Verify that the symlink exists and targets the correct Kerberos cryptographic policy with the following command:

```
$ file /etc/crypto-policies/back-ends/krb5.config
```

If command output shows the following line, Kerberos is configured to use the systemwide crypto policy:

```
/etc/crypto-policies/back-ends/krb5.config: symbolic link to
/usr/share/crypto-policies/FIPS/krb5.txt
```

If the symlink does not exist or points to a different target, this is a finding.

Remediation:

Configure Kerberos to use system cryptographic policy.
Create a symlink pointing to system crypto policy in the Kerberos configuration using the following command:

```
$ sudo ln -s /etc/crypto-policies/back-ends/krb5.config /usr/share/crypto-
policies/FIPS/krb5.txt
```

Additional Information:

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53 :: IA-7
- NIST SP 800-53 Revision 4 :: IA-7
- NIST SP 800-53 Revision 5 :: IA-7
- NIST SP 800-53A :: IA-7.1

1.452 RHEL-09-672050 (Automated)

Profile Applicability:

- SEVERITY: CAT II

Description:

RHEL 9 must implement DOD-approved encryption in the bind package.

```
GROUP ID: V-258242
RULE ID: SV-258242r958908
```

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 secret key used to generate the hash.

RHEL 9 incorporates system-wide crypto policies by default. The employed algorithms can be viewed in the /etc/crypto-policies/back-ends/ directory.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000426-GPOS-00190

Audit:

Verify that BIND uses the system crypto policy with the following command:
Note: If the "bind" package is not installed, this requirement is Not Applicable.

```
$ sudo grep include /etc/named.conf

include "/etc/crypto-policies/back-ends/bind.config";'
```

If BIND is installed and the BIND config file doesn't contain the include "/etc/crypto-policies/back-ends/bind.config" directive, or the line is commented out, this is a finding.

Remediation:

Configure BIND to use the system crypto policy.
Add the following line to the "options" section in "/etc/named.conf":

```
include "/etc/crypto-policies/back-ends/bind.config";
```

Additional Information:

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4 :: SC-8
- NIST SP 800-53 Revision 5 :: SC-8

CCI-002422 Maintain the confidentiality and/or integrity of information during reception.

- NIST SP 800-53 Revision 4 :: SC-8 (2)
- NIST SP 800-53 Revision 5 :: SC-8 (2)

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	RHEL-09-171011 (Manual)	☐	☐
1.2	RHEL-09-211010 (Manual)	☐	☐
1.3	RHEL-09-211015 (Manual)	☐	☐
1.4	RHEL-09-211020 (Manual)	☐	☐
1.5	RHEL-09-211030 (Automated)	☐	☐
1.6	RHEL-09-211035 (Automated)	☐	☐
1.7	RHEL-09-211040 (Automated)	☐	☐
1.8	RHEL-09-211045 (Automated)	☐	☐
1.9	RHEL-09-211050 (Automated)	☐	☐
1.10	RHEL-09-211055 (Automated)	☐	☐
1.11	RHEL-09-212010 (Automated)	☐	☐
1.12	RHEL-09-212015 (Automated)	☐	☐
1.13	RHEL-09-212020 (Manual)	☐	☐
1.14	RHEL-09-212025 (Automated)	☐	☐
1.15	RHEL-09-212030 (Automated)	☐	☐
1.16	RHEL-09-212035 (Automated)	☐	☐
1.17	RHEL-09-212040 (Automated)	☐	☐
1.18	RHEL-09-212045 (Automated)	☐	☐
1.19	RHEL-09-212050 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	RHEL-09-212055 (Automated)	☐	☐
1.21	RHEL-09-213010 (Automated)	☐	☐
1.22	RHEL-09-213015 (Automated)	☐	☐
1.23	RHEL-09-213020 (Automated)	☐	☐
1.24	RHEL-09-213025 (Automated)	☐	☐
1.25	RHEL-09-213030 (Automated)	☐	☐
1.26	RHEL-09-213035 (Automated)	☐	☐
1.27	RHEL-09-213040 (Manual)	☐	☐
1.28	RHEL-09-213045 (Automated)	☐	☐
1.29	RHEL-09-213050 (Automated)	☐	☐
1.30	RHEL-09-213055 (Automated)	☐	☐
1.31	RHEL-09-213060 (Automated)	☐	☐
1.32	RHEL-09-213065 (Automated)	☐	☐
1.33	RHEL-09-213070 (Automated)	☐	☐
1.34	RHEL-09-213075 (Automated)	☐	☐
1.35	RHEL-09-213080 (Automated)	☐	☐
1.36	RHEL-09-213085 (Automated)	☐	☐
1.37	RHEL-09-213090 (Automated)	☐	☐
1.38	RHEL-09-213095 (Automated)	☐	☐
1.39	RHEL-09-213100 (Automated)	☐	☐
1.40	RHEL-09-213105 (Automated)	☐	☐
1.41	RHEL-09-213110 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	RHEL-09-213115 (Automated)	☐	☐
1.43	RHEL-09-214010 (Manual)	☐	☐
1.44	RHEL-09-214015 (Automated)	☐	☐
1.45	RHEL-09-214020 (Automated)	☐	☐
1.46	RHEL-09-214025 (Automated)	☐	☐
1.47	RHEL-09-214030 (Manual)	☐	☐
1.48	RHEL-09-214035 (Automated)	☐	☐
1.49	RHEL-09-215010 (Automated)	☐	☐
1.50	RHEL-09-215015 (Automated)	☐	☐
1.51	RHEL-09-215020 (Automated)	☐	☐
1.52	RHEL-09-215025 (Automated)	☐	☐
1.53	RHEL-09-215030 (Automated)	☐	☐
1.54	RHEL-09-215035 (Automated)	☐	☐
1.55	RHEL-09-215040 (Automated)	☐	☐
1.56	RHEL-09-215045 (Automated)	☐	☐
1.57	RHEL-09-215050 (Automated)	☐	☐
1.58	RHEL-09-215055 (Automated)	☐	☐
1.59	RHEL-09-215060 (Automated)	☐	☐
1.60	RHEL-09-215065 (Automated)	☐	☐
1.61	RHEL-09-215070 (Automated)	☐	☐
1.62	RHEL-09-215075 (Automated)	☐	☐
1.63	RHEL-09-215080 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	RHEL-09-215085 (Automated)	☐	☐
1.65	RHEL-09-215090 (Automated)	☐	☐
1.66	RHEL-09-215095 (Automated)	☐	☐
1.67	RHEL-09-215100 (Automated)	☐	☐
1.68	RHEL-09-215101 (Automated)	☐	☐
1.69	RHEL-09-215105 (Manual)	☐	☐
1.70	RHEL-09-231010 (Automated)	☐	☐
1.71	RHEL-09-231015 (Automated)	☐	☐
1.72	RHEL-09-231020 (Automated)	☐	☐
1.73	RHEL-09-231025 (Automated)	☐	☐
1.74	RHEL-09-231030 (Automated)	☐	☐
1.75	RHEL-09-231035 (Automated)	☐	☐
1.76	RHEL-09-231040 (Automated)	☐	☐
1.77	RHEL-09-231045 (Automated)	☐	☐
1.78	RHEL-09-231050 (Automated)	☐	☐
1.79	RHEL-09-231055 (Automated)	☐	☐
1.80	RHEL-09-231065 (Manual)	☐	☐
1.81	RHEL-09-231070 (Manual)	☐	☐
1.82	RHEL-09-231075 (Manual)	☐	☐
1.83	RHEL-09-231080 (Manual)	☐	☐
1.84	RHEL-09-231085 (Manual)	☐	☐
1.85	RHEL-09-231090 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.86	RHEL-09-231095 (Automated)	☐	☐
1.87	RHEL-09-231100 (Automated)	☐	☐
1.88	RHEL-09-231105 (Automated)	☐	☐
1.89	RHEL-09-231110 (Automated)	☐	☐
1.90	RHEL-09-231115 (Automated)	☐	☐
1.91	RHEL-09-231120 (Automated)	☐	☐
1.92	RHEL-09-231125 (Automated)	☐	☐
1.93	RHEL-09-231130 (Automated)	☐	☐
1.94	RHEL-09-231135 (Automated)	☐	☐
1.95	RHEL-09-231140 (Automated)	☐	☐
1.96	RHEL-09-231145 (Automated)	☐	☐
1.97	RHEL-09-231150 (Automated)	☐	☐
1.98	RHEL-09-231155 (Automated)	☐	☐
1.99	RHEL-09-231160 (Automated)	☐	☐
1.100	RHEL-09-231165 (Automated)	☐	☐
1.101	RHEL-09-231170 (Automated)	☐	☐
1.102	RHEL-09-231175 (Automated)	☐	☐
1.103	RHEL-09-231180 (Automated)	☐	☐
1.104	RHEL-09-231185 (Automated)	☐	☐
1.105	RHEL-09-231190 (Manual)	☐	☐
1.106	RHEL-09-231195 (Automated)	☐	☐
1.107	RHEL-09-231200 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.108	RHEL-09-232010 (Automated)	☐	☐
1.109	RHEL-09-232015 (Automated)	☐	☐
1.110	RHEL-09-232020 (Automated)	☐	☐
1.111	RHEL-09-232025 (Automated)	☐	☐
1.112	RHEL-09-232030 (Automated)	☐	☐
1.113	RHEL-09-232035 (Automated)	☐	☐
1.114	RHEL-09-232040 (Manual)	☐	☐
1.115	RHEL-09-232045 (Manual)	☐	☐
1.116	RHEL-09-232050 (Manual)	☐	☐
1.117	RHEL-09-232055 (Automated)	☐	☐
1.118	RHEL-09-232060 (Automated)	☐	☐
1.119	RHEL-09-232065 (Automated)	☐	☐
1.120	RHEL-09-232070 (Automated)	☐	☐
1.121	RHEL-09-232075 (Automated)	☐	☐
1.122	RHEL-09-232080 (Automated)	☐	☐
1.123	RHEL-09-232085 (Automated)	☐	☐
1.124	RHEL-09-232090 (Automated)	☐	☐
1.125	RHEL-09-232095 (Automated)	☐	☐
1.126	RHEL-09-232100 (Automated)	☐	☐
1.127	RHEL-09-232103 (Automated)	☐	☐
1.128	RHEL-09-232104 (Automated)	☐	☐
1.129	RHEL-09-232105 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.130	RHEL-09-232110 (Automated)	☐	☐
1.131	RHEL-09-232115 (Automated)	☐	☐
1.132	RHEL-09-232120 (Automated)	☐	☐
1.133	RHEL-09-232125 (Automated)	☐	☐
1.134	RHEL-09-232130 (Automated)	☐	☐
1.135	RHEL-09-232135 (Automated)	☐	☐
1.136	RHEL-09-232140 (Automated)	☐	☐
1.137	RHEL-09-232145 (Automated)	☐	☐
1.138	RHEL-09-232150 (Automated)	☐	☐
1.139	RHEL-09-232155 (Automated)	☐	☐
1.140	RHEL-09-232160 (Automated)	☐	☐
1.141	RHEL-09-232165 (Automated)	☐	☐
1.142	RHEL-09-232170 (Automated)	☐	☐
1.143	RHEL-09-232175 (Automated)	☐	☐
1.144	RHEL-09-232180 (Automated)	☐	☐
1.145	RHEL-09-232185 (Automated)	☐	☐
1.146	RHEL-09-232190 (Automated)	☐	☐
1.147	RHEL-09-232195 (Automated)	☐	☐
1.148	RHEL-09-232200 (Automated)	☐	☐
1.149	RHEL-09-232205 (Automated)	☐	☐
1.150	RHEL-09-232210 (Automated)	☐	☐
1.151	RHEL-09-232215 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.152	RHEL-09-232220 (Automated)	☐	☐
1.153	RHEL-09-232225 (Automated)	☐	☐
1.154	RHEL-09-232230 (Automated)	☐	☐
1.155	RHEL-09-232235 (Automated)	☐	☐
1.156	RHEL-09-232240 (Manual)	☐	☐
1.157	RHEL-09-232245 (Automated)	☐	☐
1.158	RHEL-09-232250 (Automated)	☐	☐
1.159	RHEL-09-232255 (Automated)	☐	☐
1.160	RHEL-09-232260 (Manual)	☐	☐
1.161	RHEL-09-232270 (Automated)	☐	☐
1.162	RHEL-09-251010 (Automated)	☐	☐
1.163	RHEL-09-251015 (Automated)	☐	☐
1.164	RHEL-09-251020 (Manual)	☐	☐
1.165	RHEL-09-251030 (Automated)	☐	☐
1.166	RHEL-09-251035 (Manual)	☐	☐
1.167	RHEL-09-251040 (Manual)	☐	☐
1.168	RHEL-09-251045 (Automated)	☐	☐
1.169	RHEL-09-252010 (Automated)	☐	☐
1.170	RHEL-09-252015 (Automated)	☐	☐
1.171	RHEL-09-252020 (Automated)	☐	☐
1.172	RHEL-09-252025 (Automated)	☐	☐
1.173	RHEL-09-252030 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.174	RHEL-09-252035 (Manual)	☐	☐
1.175	RHEL-09-252040 (Manual)	☐	☐
1.176	RHEL-09-252045 (Automated)	☐	☐
1.177	RHEL-09-252050 (Automated)	☐	☐
1.178	RHEL-09-252060 (Automated)	☐	☐
1.179	RHEL-09-252065 (Automated)	☐	☐
1.180	RHEL-09-252070 (Manual)	☐	☐
1.181	RHEL-09-252075 (Manual)	☐	☐
1.182	RHEL-09-253010 (Automated)	☐	☐
1.183	RHEL-09-253015 (Automated)	☐	☐
1.184	RHEL-09-253020 (Automated)	☐	☐
1.185	RHEL-09-253025 (Automated)	☐	☐
1.186	RHEL-09-253030 (Automated)	☐	☐
1.187	RHEL-09-253035 (Automated)	☐	☐
1.188	RHEL-09-253040 (Automated)	☐	☐
1.189	RHEL-09-253045 (Automated)	☐	☐
1.190	RHEL-09-253050 (Automated)	☐	☐
1.191	RHEL-09-253055 (Automated)	☐	☐
1.192	RHEL-09-253060 (Automated)	☐	☐
1.193	RHEL-09-253065 (Automated)	☐	☐
1.194	RHEL-09-253070 (Automated)	☐	☐
1.195	RHEL-09-253075 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.196	RHEL-09-254010 (Automated)	☐	☐
1.197	RHEL-09-254015 (Automated)	☐	☐
1.198	RHEL-09-254020 (Automated)	☐	☐
1.199	RHEL-09-254025 (Automated)	☐	☐
1.200	RHEL-09-254030 (Automated)	☐	☐
1.201	RHEL-09-254035 (Automated)	☐	☐
1.202	RHEL-09-254040 (Automated)	☐	☐
1.203	RHEL-09-255010 (Automated)	☐	☐
1.204	RHEL-09-255015 (Automated)	☐	☐
1.205	RHEL-09-255020 (Automated)	☐	☐
1.206	RHEL-09-255025 (Automated)	☐	☐
1.207	RHEL-09-255030 (Automated)	☐	☐
1.208	RHEL-09-255035 (Automated)	☐	☐
1.209	RHEL-09-255040 (Automated)	☐	☐
1.210	RHEL-09-255045 (Automated)	☐	☐
1.211	RHEL-09-255050 (Automated)	☐	☐
1.212	RHEL-09-255055 (Automated)	☐	☐
1.213	RHEL-09-255060 (Automated)	☐	☐
1.214	RHEL-09-255064 (Manual)	☐	☐
1.215	RHEL-09-255065 (Manual)	☐	☐
1.216	RHEL-09-255070 (Manual)	☐	☐
1.217	RHEL-09-255075 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.218	RHEL-09-255080 (Automated)	☐	☐
1.219	RHEL-09-255085 (Automated)	☐	☐
1.220	RHEL-09-255090 (Automated)	☐	☐
1.221	RHEL-09-255095 (Automated)	☐	☐
1.222	RHEL-09-255100 (Automated)	☐	☐
1.223	RHEL-09-255105 (Automated)	☐	☐
1.224	RHEL-09-255110 (Automated)	☐	☐
1.225	RHEL-09-255115 (Manual)	☐	☐
1.226	RHEL-09-255120 (Automated)	☐	☐
1.227	RHEL-09-255125 (Automated)	☐	☐
1.228	RHEL-09-255130 (Automated)	☐	☐
1.229	RHEL-09-255135 (Automated)	☐	☐
1.230	RHEL-09-255140 (Automated)	☐	☐
1.231	RHEL-09-255145 (Automated)	☐	☐
1.232	RHEL-09-255150 (Automated)	☐	☐
1.233	RHEL-09-255155 (Automated)	☐	☐
1.234	RHEL-09-255160 (Automated)	☐	☐
1.235	RHEL-09-255165 (Automated)	☐	☐
1.236	RHEL-09-255175 (Automated)	☐	☐
1.237	RHEL-09-271010 (Automated)	☐	☐
1.238	RHEL-09-271015 (Automated)	☐	☐
1.239	RHEL-09-271020 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.240	RHEL-09-271025 (Manual)	☐	☐
1.241	RHEL-09-271030 (Automated)	☐	☐
1.242	RHEL-09-271035 (Automated)	☐	☐
1.243	RHEL-09-271040 (Automated)	☐	☐
1.244	RHEL-09-271045 (Automated)	☐	☐
1.245	RHEL-09-271050 (Automated)	☐	☐
1.246	RHEL-09-271055 (Automated)	☐	☐
1.247	RHEL-09-271060 (Automated)	☐	☐
1.248	RHEL-09-271065 (Automated)	☐	☐
1.249	RHEL-09-271070 (Automated)	☐	☐
1.250	RHEL-09-271075 (Automated)	☐	☐
1.251	RHEL-09-271080 (Automated)	☐	☐
1.252	RHEL-09-271085 (Automated)	☐	☐
1.253	RHEL-09-271090 (Manual)	☐	☐
1.254	RHEL-09-271095 (Automated)	☐	☐
1.255	RHEL-09-271100 (Automated)	☐	☐
1.256	RHEL-09-271105 (Manual)	☐	☐
1.257	RHEL-09-271110 (Automated)	☐	☐
1.258	RHEL-09-271115 (Automated)	☐	☐
1.259	RHEL-09-291010 (Automated)	☐	☐
1.260	RHEL-09-291015 (Automated)	☐	☐
1.261	RHEL-09-291020 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.262	RHEL-09-291025 (Automated)	☐	☐
1.263	RHEL-09-291030 (Manual)	☐	☐
1.264	RHEL-09-291035 (Automated)	☐	☐
1.265	RHEL-09-291040 (Automated)	☐	☐
1.266	RHEL-09-411010 (Automated)	☐	☐
1.267	RHEL-09-411015 (Automated)	☐	☐
1.268	RHEL-09-411020 (Automated)	☐	☐
1.269	RHEL-09-411025 (Manual)	☐	☐
1.270	RHEL-09-411030 (Automated)	☐	☐
1.271	RHEL-09-411035 (Automated)	☐	☐
1.272	RHEL-09-411040 (Manual)	☐	☐
1.273	RHEL-09-411045 (Automated)	☐	☐
1.274	RHEL-09-411050 (Automated)	☐	☐
1.275	RHEL-09-411055 (Automated)	☐	☐
1.276	RHEL-09-411060 (Automated)	☐	☐
1.277	RHEL-09-411065 (Automated)	☐	☐
1.278	RHEL-09-411070 (Automated)	☐	☐
1.279	RHEL-09-411075 (Automated)	☐	☐
1.280	RHEL-09-411080 (Automated)	☐	☐
1.281	RHEL-09-411085 (Automated)	☐	☐
1.282	RHEL-09-411090 (Automated)	☐	☐
1.283	RHEL-09-411095 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.284	RHEL-09-411100 (Automated)	☐	☐
1.285	RHEL-09-411105 (Automated)	☐	☐
1.286	RHEL-09-411110 (Automated)	☐	☐
1.287	RHEL-09-411115 (Automated)	☐	☐
1.288	RHEL-09-412035 (Automated)	☐	☐
1.289	RHEL-09-412040 (Automated)	☐	☐
1.290	RHEL-09-412045 (Automated)	☐	☐
1.291	RHEL-09-412050 (Automated)	☐	☐
1.292	RHEL-09-412055 (Automated)	☐	☐
1.293	RHEL-09-412060 (Automated)	☐	☐
1.294	RHEL-09-412065 (Automated)	☐	☐
1.295	RHEL-09-412070 (Automated)	☐	☐
1.296	RHEL-09-412075 (Automated)	☐	☐
1.297	RHEL-09-412080 (Automated)	☐	☐
1.298	RHEL-09-431010 (Automated)	☐	☐
1.299	RHEL-09-431015 (Automated)	☐	☐
1.300	RHEL-09-431016 (Manual)	☐	☐
1.301	RHEL-09-431020 (Automated)	☐	☐
1.302	RHEL-09-431025 (Automated)	☐	☐
1.303	RHEL-09-431030 (Automated)	☐	☐
1.304	RHEL-09-432010 (Automated)	☐	☐
1.305	RHEL-09-432015 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.306	RHEL-09-432020 (Manual)	☐	☐
1.307	RHEL-09-432025 (Automated)	☐	☐
1.308	RHEL-09-432030 (Automated)	☐	☐
1.309	RHEL-09-432035 (Automated)	☐	☐
1.310	RHEL-09-433010 (Automated)	☐	☐
1.311	RHEL-09-433015 (Automated)	☐	☐
1.312	RHEL-09-433016 (Manual)	☐	☐
1.313	RHEL-09-611010 (Automated)	☐	☐
1.314	RHEL-09-611025 (Automated)	☐	☐
1.315	RHEL-09-611030 (Automated)	☐	☐
1.316	RHEL-09-611035 (Automated)	☐	☐
1.317	RHEL-09-611040 (Automated)	☐	☐
1.318	RHEL-09-611045 (Automated)	☐	☐
1.319	RHEL-09-611050 (Automated)	☐	☐
1.320	RHEL-09-611055 (Automated)	☐	☐
1.321	RHEL-09-611060 (Automated)	☐	☐
1.322	RHEL-09-611065 (Automated)	☐	☐
1.323	RHEL-09-611070 (Automated)	☐	☐
1.324	RHEL-09-611075 (Automated)	☐	☐
1.325	RHEL-09-611080 (Automated)	☐	☐
1.326	RHEL-09-611085 (Automated)	☐	☐
1.327	RHEL-09-611090 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.328	RHEL-09-611100 (Automated)	☐	☐
1.329	RHEL-09-611105 (Automated)	☐	☐
1.330	RHEL-09-611110 (Automated)	☐	☐
1.331	RHEL-09-611115 (Automated)	☐	☐
1.332	RHEL-09-611120 (Automated)	☐	☐
1.333	RHEL-09-611125 (Automated)	☐	☐
1.334	RHEL-09-611130 (Automated)	☐	☐
1.335	RHEL-09-611135 (Automated)	☐	☐
1.336	RHEL-09-611140 (Automated)	☐	☐
1.337	RHEL-09-611145 (Automated)	☐	☐
1.338	RHEL-09-611155 (Automated)	☐	☐
1.339	RHEL-09-611160 (Manual)	☐	☐
1.340	RHEL-09-611165 (Automated)	☐	☐
1.341	RHEL-09-611170 (Automated)	☐	☐
1.342	RHEL-09-611175 (Automated)	☐	☐
1.343	RHEL-09-611180 (Automated)	☐	☐
1.344	RHEL-09-611185 (Automated)	☐	☐
1.345	RHEL-09-611190 (Manual)	☐	☐
1.346	RHEL-09-611195 (Automated)	☐	☐
1.347	RHEL-09-611200 (Automated)	☐	☐
1.348	RHEL-09-631010 (Manual)	☐	☐
1.349	RHEL-09-631015 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.350	RHEL-09-631020 (Manual)	☐	☐
1.351	RHEL-09-651010 (Automated)	☐	☐
1.352	RHEL-09-651015 (Automated)	☐	☐
1.353	RHEL-09-651020 (Manual)	☐	☐
1.354	RHEL-09-651025 (Automated)	☐	☐
1.355	RHEL-09-651030 (Manual)	☐	☐
1.356	RHEL-09-651035 (Manual)	☐	☐
1.357	RHEL-09-652010 (Automated)	☐	☐
1.358	RHEL-09-652015 (Automated)	☐	☐
1.359	RHEL-09-652020 (Automated)	☐	☐
1.360	RHEL-09-652025 (Manual)	☐	☐
1.361	RHEL-09-652030 (Automated)	☐	☐
1.362	RHEL-09-652040 (Automated)	☐	☐
1.363	RHEL-09-652045 (Automated)	☐	☐
1.364	RHEL-09-652050 (Automated)	☐	☐
1.365	RHEL-09-652055 (Manual)	☐	☐
1.366	RHEL-09-652060 (Automated)	☐	☐
1.367	RHEL-09-653010 (Automated)	☐	☐
1.368	RHEL-09-653015 (Automated)	☐	☐
1.369	RHEL-09-653020 (Automated)	☐	☐
1.370	RHEL-09-653025 (Automated)	☐	☐
1.371	RHEL-09-653030 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.372	RHEL-09-653035 (Automated)	☐	☐
1.373	RHEL-09-653040 (Automated)	☐	☐
1.374	RHEL-09-653045 (Automated)	☐	☐
1.375	RHEL-09-653050 (Automated)	☐	☐
1.376	RHEL-09-653055 (Automated)	☐	☐
1.377	RHEL-09-653060 (Automated)	☐	☐
1.378	RHEL-09-653065 (Automated)	☐	☐
1.379	RHEL-09-653070 (Automated)	☐	☐
1.380	RHEL-09-653075 (Automated)	☐	☐
1.381	RHEL-09-653080 (Automated)	☐	☐
1.382	RHEL-09-653085 (Automated)	☐	☐
1.383	RHEL-09-653090 (Automated)	☐	☐
1.384	RHEL-09-653095 (Automated)	☐	☐
1.385	RHEL-09-653100 (Automated)	☐	☐
1.386	RHEL-09-653105 (Automated)	☐	☐
1.387	RHEL-09-653110 (Automated)	☐	☐
1.388	RHEL-09-653115 (Automated)	☐	☐
1.389	RHEL-09-653120 (Automated)	☐	☐
1.390	RHEL-09-653125 (Manual)	☐	☐
1.391	RHEL-09-653130 (Automated)	☐	☐
1.392	RHEL-09-654010 (Automated)	☐	☐
1.393	RHEL-09-654015 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.394	RHEL-09-654020 (Automated)	☐	☐
1.395	RHEL-09-654025 (Automated)	☐	☐
1.396	RHEL-09-654030 (Automated)	☐	☐
1.397	RHEL-09-654035 (Automated)	☐	☐
1.398	RHEL-09-654040 (Automated)	☐	☐
1.399	RHEL-09-654045 (Automated)	☐	☐
1.400	RHEL-09-654050 (Automated)	☐	☐
1.401	RHEL-09-654055 (Automated)	☐	☐
1.402	RHEL-09-654060 (Automated)	☐	☐
1.403	RHEL-09-654065 (Automated)	☐	☐
1.404	RHEL-09-654070 (Automated)	☐	☐
1.405	RHEL-09-654075 (Automated)	☐	☐
1.406	RHEL-09-654080 (Automated)	☐	☐
1.407	RHEL-09-654085 (Automated)	☐	☐
1.408	RHEL-09-654090 (Automated)	☐	☐
1.409	RHEL-09-654095 (Automated)	☐	☐
1.410	RHEL-09-654100 (Automated)	☐	☐
1.411	RHEL-09-654105 (Automated)	☐	☐
1.412	RHEL-09-654110 (Automated)	☐	☐
1.413	RHEL-09-654115 (Automated)	☐	☐
1.414	RHEL-09-654120 (Automated)	☐	☐
1.415	RHEL-09-654125 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.416	RHEL-09-654130 (Automated)	☐	☐
1.417	RHEL-09-654135 (Automated)	☐	☐
1.418	RHEL-09-654140 (Automated)	☐	☐
1.419	RHEL-09-654145 (Automated)	☐	☐
1.420	RHEL-09-654150 (Automated)	☐	☐
1.421	RHEL-09-654155 (Automated)	☐	☐
1.422	RHEL-09-654160 (Automated)	☐	☐
1.423	RHEL-09-654165 (Automated)	☐	☐
1.424	RHEL-09-654170 (Automated)	☐	☐
1.425	RHEL-09-654175 (Automated)	☐	☐
1.426	RHEL-09-654180 (Automated)	☐	☐
1.427	RHEL-09-654185 (Automated)	☐	☐
1.428	RHEL-09-654190 (Automated)	☐	☐
1.429	RHEL-09-654195 (Automated)	☐	☐
1.430	RHEL-09-654200 (Automated)	☐	☐
1.431	RHEL-09-654205 (Automated)	☐	☐
1.432	RHEL-09-654210 (Automated)	☐	☐
1.433	RHEL-09-654215 (Automated)	☐	☐
1.434	RHEL-09-654220 (Automated)	☐	☐
1.435	RHEL-09-654225 (Automated)	☐	☐
1.436	RHEL-09-654230 (Automated)	☐	☐
1.437	RHEL-09-654235 (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.438	RHEL-09-654240 (Automated)	☐	☐
1.439	RHEL-09-654245 (Automated)	☐	☐
1.440	RHEL-09-654250 (Automated)	☐	☐
1.441	RHEL-09-654255 (Automated)	☐	☐
1.442	RHEL-09-654260 (Automated)	☐	☐
1.443	RHEL-09-654265 (Automated)	☐	☐
1.444	RHEL-09-654270 (Automated)	☐	☐
1.445	RHEL-09-654275 (Automated)	☐	☐
1.446	RHEL-09-671010 (Automated)	☐	☐
1.447	RHEL-09-671015 (Automated)	☐	☐
1.448	RHEL-09-671020 (Automated)	☐	☐
1.449	RHEL-09-671025 (Automated)	☐	☐
1.450	RHEL-09-672020 (Manual)	☐	☐
1.451	RHEL-09-672025 (Manual)	☐	☐
1.452	RHEL-09-672050 (Automated)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Apr 29, 2025	1.0.0	PUBLISHED