CIS Center for Internet Security®

CIS Benchmarks™

CIS Oracle Linux 7 STIG Benchmark

v1.0.0 - 08-22-2025

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

Target Technology Details

Oracle Linux 7 Secure Technical Implementation Guide (STIG)

Version: 3 Release: 3 Benchmark

Date: 02 Jul 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 Oracle Linux 7 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 (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG.

Rationale Statement

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

Additional Information

References from the STIG Rule if applicable.

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

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Oracle Linux 7

Recommendations

1 STIG RULES

Oracle Linux 7

Oracle Linux 7 Secure Technical Implementation Guide (STIG)

Version: 3 Release: 3 Benchmark

Date: 02 Jul 2025

CLASSIFICATION unclassified

1.1 OL07-00-010010 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must be configured so that the file permissions, ownership, and group membership of system files and commands match the vendor values.

```
GROUP ID: V-221652
RULE ID: SV-221652r991557
```

Rationale:

Discretionary access control is weakened if a user or group has access permissions to system files and directories greater than the default.

Satisfies: SRG-OS-000257-GPOS-00098, SRG-OS-000278-GPOS-00108

Audit:

Verify the file permissions, ownership, and group membership of system files and commands match the vendor values.

Check the default file permissions, ownership, and group membership of system files and commands with the following command:

```
 # for i in `rpm -Va | grep -E '^.{1}M|^.{5}U|^.{6}G' | cut -d " " -f 4,5`;do
for j in `rpm -qf $i`;do rpm -ql $j --dump | cut -d " " -f 1,5,6,7 | grep
$i;done;done

 /var/log/gdm 040755 root root
 /etc/audisp/audisp-remote.conf 0100640 root root
 /usr/bin/passwd 0104755 root root
```

For each file returned, verify the current permissions, ownership, and group membership:

ls -la

```
 -rw-------. 1 root root  2017 Nov 1 10:03 /etc/audisp/audisp-remote.conf
```

If the file is more permissive than the default permissions, this is a finding.

If the file is not owned by the default owner and is not documented with the Information System Security Officer (ISSO), this is a finding.

If the file is not a member of the default group and is not documented with the ISSO, this is a finding.

Remediation:

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

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

Reset the user and group ownership of files within a package with the following command:

```
# rpm --setugids <packagename>
```

Reset the permissions of files within a package with the following command:

```
# rpm --setperms <packagename>
```

Additional Information:

CCI-001494 Protect audit tools from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001496 Implement cryptographic mechanisms to protect the integrity of audit tools.

- NIST SP 800-53::AU-9 (3)
- NIST SP 800-53A::AU-9 (3).1
- NIST SP 800-53 Revision 4::AU-9 (3)
- NIST SP 800-53 Revision 5::AU-9 (3)

1.2 OL07-00-010019 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must ensure cryptographic verification of vendor software packages.

```
GROUP ID: V-256975
RULE ID: SV-256975r1015198
```

Rationale:

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

Audit:

Confirm Oracle package-signing key is installed on the system and verify its fingerprint matches vendor value.

Note: The GPG key is defined in key file "/etc/pki/rpm-gpg/RPM-GPG-KEY-oracle" by default.

List Oracle GPG keys installed on the system:

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

 gpg(Oracle OSS group (Open Source Software group) <build@oss.oracle.com>)
```

If Oracle GPG key is not installed, this is a finding.

List key fingerprint of installed Oracle GPG key:

```
 $ sudo gpg -q --with-fingerprint /etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
```

If key file "/etc/pki/rpm-gpg/RPM-GPG-KEY-oracle" is missing, this is a finding.

Example output:

```
 pub  2048R/EC551F03 2010-07-01 Oracle OSS group (Open Source Software group)
<build@oss.oracle.com>
       Key fingerprint = 4214 4123 FECF C55B 9086  313D 72F9 7B74 EC55 1F03
```

Compare key fingerprint of installed Oracle GPG key with fingerprint listed for OL 7 on Oracle verification webpage at https://linux.oracle.com/security/gpg/#gpg.

If key fingerprint does not match, this is a finding.

Remediation:

Install Oracle package-signing key on the system and verify its fingerprint matches vendor value.

Insert OL 7 installation disc or attach OL 7 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 Oracle GPG key file onto the system:

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

Import Oracle GPG keys from key file into system keyring:

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

Using the steps listed in the Check Text, confirm the newly imported key shows as installed on the system and verify its fingerprint matches vendor value.

Additional Information:

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)

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

1.3 OL07-00-010020 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must be configured so that the cryptographic hash of system files and commands matches vendor values.

```
GROUP ID: V-221653
RULE ID: SV-221653r1015161
```

Rationale:

Without cryptographic integrity protections, system command and files can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Audit:

Verify the cryptographic hash of system files and commands match the vendor values.

Check the cryptographic hash of system files and commands with the following command:

Note: System configuration files (indicated by a "c" in the second column) are expected to change over time. Unusual modifications should be investigated through the system audit log.

```
# rpm -Va --noconfig | grep '^..5'
```

If there is any output from the command for system files or binaries, this is a finding.

Remediation:

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

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

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

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

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

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

Additional Information:

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)

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

1.4 OL07-00-010030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system 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-221654
RULE ID: SV-221654r958390
```

Rationale:

The 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-000024-GPOS-00007, SRG-OS-000228-GPOS-00088

Audit:

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

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

Check to see if the operating system displays a banner at the logon screen with the following command:

```
# grep banner-message-enable /etc/dconf/db/local.d/*
banner-message-enable=true
```

If "banner-message-enable" is set to "false" or is missing, 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.

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

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

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

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

```
[org/gnome/login-screen]
banner-message-enable=true
```

Update the system databases:

```
# dconf update
```

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

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

CCI-000050 Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system.

- NIST SP 800-53::AC-8 b
- NIST SP 800-53A::AC-8.1 (iii)
- NIST SP 800-53 Revision 4::AC-8 b
- NIST SP 800-53 Revision 5::AC-8 b

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

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

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

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

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

1.5 OL07-00-010040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221655
RULE ID: SV-221655r958390
```

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.

"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-000024-GPOS-00007, SRG-OS-000228-GPOS-00088

Audit:

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

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

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

```
# grep banner-message-text /etc/dconf/db/local.d/*
banner-message-text=
'You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only.\nBy using this IS (which includes any
device attached to this IS), you consent to the following conditions:\n-The
USG routinely intercepts and monitors communications on this IS for purposes
including, but not limited to, penetration testing, COMSEC monitoring,
network operations and defense, personnel misconduct (PM), law enforcement
(LE), and counterintelligence (CI) investigations.\n-At any time, the USG may
inspect and seize data stored on this IS.\n-Communications using, or data
stored on, this IS are not private, are subject to routine monitoring,
interception, and search, and may be disclosed or used for any USG-authorized
purpose.\n-This IS includes security measures (e.g., authentication and
access controls) to protect USG interests--not for your personal benefit or
privacy.\n-Notwithstanding the above, using this IS does not constitute
consent to PM, LE or CI investigative searching or monitoring of the content
of privileged communications, or work product, related to personal
representation or services by attorneys, psychotherapists, or clergy, and
their assistants. Such communications and work product are private and
confidential. See User Agreement for details.'
```

Note: The "\n" characters are for formatting only. They will not be displayed on the Graphical User Interface.

If the banner does not match the approved Standard Mandatory DoD Notice and Consent Banner, this is a finding.

Remediation:

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

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

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

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

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

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

banner-message-enable=true
banner-message-text='You are accessing a U.S. Government (USG) Information
System (IS) that is provided for USG-authorized use only.\nBy using this IS
(which includes any device attached to this IS), you consent to the following
conditions:\n-The USG routinely intercepts and monitors communications on
this IS for purposes including, but not limited to, penetration testing,
COMSEC monitoring, network operations and defense, personnel misconduct (PM),
law enforcement (LE), and counterintelligence (CI) investigations.\n-At any
time, the USG may inspect and seize data stored on this IS.\n-Communications
using, or data stored on, this IS are not private, are subject to routine
monitoring, interception, and search, and may be disclosed or used for any
USG-authorized purpose.\n-This IS includes security measures (e.g.,
authentication and access controls) to protect USG interests--not for your
personal benefit or privacy.\n-Notwithstanding the above, using this IS does
not constitute consent to PM, LE or CI investigative searching or monitoring
of the content of privileged communications, or work product, related to
personal representation or services by attorneys, psychotherapists, or
clergy, and their assistants. Such communications and work product are
private and confidential. See User Agreement for details.'
```

Note: The "\n" characters are for formatting only. They will not be displayed on the Graphical User Interface.

Run the following command to update the database:

```
# dconf update
```

Additional Information:

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

1.6 OL07-00-010050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting local or remote access to the system via a command line user logon.

```
GROUP ID: V-221656
RULE ID: SV-221656r958390
```

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-000024-GPOS-00007

Audit:

Verify the operating system displays the Standard Mandatory DoD Notice and Consent Banner before granting access to the operating system via a command line user logon.

Check to see if the operating system displays a banner at the command line logon screen with the following command:

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

The command should 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 operating system does not display a graphical logon banner or the banner does not match the Standard Mandatory DoD Notice and Consent Banner, this is a finding.

If the text in the "/etc/issue" file does not match the Standard Mandatory DoD Notice and Consent Banner, this is a finding.

Remediation:

Configure the operating system to display the Standard Mandatory DoD Notice and Consent Banner before granting access to the system via the command line by editing the "/etc/issue" file.

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

1.7 OL07-00-010060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221657
RULE ID: SV-221657r1015162
```

Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

Regardless of where the session lock is determined and implemented, once invoked, the session lock must remain in place until the user reauthenticates. No other activity aside from reauthentication must unlock the system.

Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000030-GPOS-00011

Audit:

Verify the operating system enables a user's session lock until that user re-establishes access using established identification and authentication procedures.

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

Check to see if the screen lock is enabled with the following command:

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

If the "lock-enabled" setting is missing or is not set to "true", this is a finding.

Remediation:

Configure the operating system to enable a user's session lock until that user re-establishes access using established identification and authentication procedures.

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

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

Edit the "[org/gnome/desktop/screensaver]" section of the database file and add or update the following lines:

```
# Set this to true to lock the screen when the screensaver activates
lock-enabled=true
```

Update the system databases:

```
# dconf update
```

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

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 800-53A::AC-11.1 (iii)
- NIST SP 800-53 Revision 4::AC-11 b
- NIST SP 800-53 Revision 5::AC-11 b

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 800-53A::AC-11
- NIST SP 800-53 Revision 4::AC-11 a

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

1.8 OL07-00-010062 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must prevent a user from overriding the screensaver lock-enabled setting for the graphical user interface.

```
GROUP ID: V-221659
RULE ID: SV-221659r958402
```

Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

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

Audit:

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

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

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

grep system-db /etc/dconf/profile/user

```
 system-db:local
```

Check for the lock-enabled setting with the following command:

Note: The example below is using the database "local" for the system, so the path is "/etc/dconf/db/local.d". This path must be modified if a database other than "local" is being used.

```
 # grep -i lock-enabled /etc/dconf/db/local.d/locks/*

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

If the command does not return a result, this is a finding.

Remediation:

Configure the operating system to prevent a user from overriding a screensaver lock after a 15-minute period of inactivity for graphical user interfaces.

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

Note: The example below is using the database "local" for the system, so if the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
# touch /etc/dconf/db/local.d/locks/session
```

Add the setting to lock the screensaver lock-enabled setting:

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

Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

1.9 OL07-00-010061 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221658
RULE ID: SV-221658r1015163
```

Rationale:

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

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

Satisfies: SRG-OS-000375-GPOS-00161, SRG-OS-000377-GPOS-00162

Audit:

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

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

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

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

system-db:local
```

Note: The example is using the database local for the system, so the path is "/etc/dconf/db/local.d". This path must be modified if a database other than local is being used.

```
# grep enable-smartcard-authentication /etc/dconf/db/local.d/*

enable-smartcard-authentication=true
```

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

Remediation:

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

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

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

Note: The example is using the local system database, so if the system is using another database in "/etc/dconf/profile/user", create the file under the appropriate subdirectory.

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

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

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

Update the system databases:

```
# dconf update
```

Additional Information:

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)

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)

1.10 OL07-00-010063 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must disable the login screen user list for graphical user interfaces.

```
GROUP ID: V-256976
RULE ID: SV-256976r991589
```

Rationale:

Leaving the user list enabled is a security risk as it allows anyone with physical access to the system to enumerate known user accounts without authenticated access to the system.

Audit:

Verify that the operating system is configured to disable the login screen user list for graphical user interfaces.

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

Verify that the login screen user list for the GNOME Desktop is disabled with the following command:

```
 $ sudo grep -is disable-user-list /etc/dconf/db/gdm.d/*

 /etc/dconf/db/gdm.d/00-login-screen:disable-user-list=true
```

If the variable "disable-user-list" is not defined in a file under "/etc/dconf/db/gdm.d/", is not set to "true", is missing or commented out, this is a finding.

Remediation:

Configure the operating system to disable the login screen user list for graphical user interfaces.

Create or edit the gdm profile in "/etc/dconf/profile/" to contain the following lines:

```
$ sudo vi /etc/dconf/profile/gdm

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

Create or edit the gdm database for machine-wide settings in "/etc/dconf/db/gdm.d/" with the following lines:

```
$ sudo vi /etc/dconf/db/gdm.d/00-login-screen

[org/gnome/login-screen]
disable-user-list=true
```

Update the system databases by updating the dconf utility:

```
$ sudo dconf update
```

If the login screen user list persists after updating the system databases, you can restart the GNOME Desktop without rebooting the system:

```
$ sudo systemctl restart gdm
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.11 OL07-00-010070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221660
RULE ID: SV-221660r958402
```

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 lock the operating system session manually prior to leaving the workstation, operating systems must be able to identify when a user's session has idled, and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Audit:

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

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

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

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

If the "idle-delay" setting is missing or is not set to "900" or less, this is a finding.

Remediation:

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

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

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

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

```
[org/gnome/desktop/session]
# Set the lock time out to 900 seconds before the session is considered idle
idle-delay=uint32 900
```

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

Update the system databases:

```
# dconf update
```

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

Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

1.12 OL07-00-010081 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must prevent a user from overriding the screensaver lock-delay setting for the graphical user interface.

```
GROUP ID: V-221661
RULE ID: SV-221661r958402
```

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 lock the operating system session manually prior to leaving the workstation, operating systems must be able to identify when a user's session has idled, and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Audit:

Verify the operating system prevents a user from overriding a screensaver lock after a 15-minute period of inactivity for graphical user interfaces.

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

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

grep system-db /etc/dconf/profile/user

system-db:local

Check for the lock delay setting with the following command:

Note: The example below is using the database "local" for the system, so the path is "/etc/dconf/db/local.d". This path must be modified if a database other than "local" is being used.

```
 # grep -i lock-delay /etc/dconf/db/local.d/locks/*
 /org/gnome/desktop/screensaver/lock-delay
```

If the command does not return a result, this is a finding.

Remediation:

Configure the operating system to prevent a user from overriding a screensaver lock after a 15-minute period of inactivity for graphical user interfaces.

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

Note: The example below is using the database "local" for the system, so if the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
# touch /etc/dconf/db/local.d/locks/session
```

Add the setting to lock the screensaver lock delay:

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

Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

1.13 OL07-00-010082 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must prevent a user from overriding the session idle-delay setting for the graphical user interface.

```
GROUP ID: V-221662
RULE ID: SV-221662r958402
```

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 lock their operating system session manually prior to leaving the workstation, operating systems must be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Audit:

Verify the operating system prevents a user from overriding session idle delay after a 15-minute period of inactivity for graphical user interfaces.

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

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

grep system-db /etc/dconf/profile/user

system-db:local

Check for the session idle delay setting with the following command:

Note: The example below is using the database "local" for the system, so the path is "/etc/dconf/db/local.d". This path must be modified if a database other than "local" is being used.

```
 # grep -i idle-delay /etc/dconf/db/local.d/locks/*
 /org/gnome/desktop/session/idle-delay
```

If the command does not return a result, this is a finding.

Remediation:

Configure the operating system to prevent a user from overriding a session lock after a 15-minute period of inactivity for graphical user interfaces.

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

Note: The example below is using the database "local" for the system, so if the system is using another database in /etc/dconf/profile/user, the file should be created under the appropriate subdirectory.

```
# touch /etc/dconf/db/local.d/locks/session
```

Add the setting to lock the session idle delay:

```
/org/gnome/desktop/session/idle-delay
```

Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

1.14 OL07-00-010100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must initiate a session lock for the screensaver after a period of inactivity for graphical user interfaces.

```
GROUP ID: V-221664
RULE ID: SV-221664r958402
```

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 must be able to identify when a user's session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Audit:

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

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

Check for the session lock settings with the following commands:

```
 # grep -i idle-activation-enabled /etc/dconf/db/local.d/*
 idle-activation-enabled=true
```

If "idle-activation-enabled" is not set to "true", this is a finding.

Remediation:

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

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

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

Add the setting to enable screensaver locking after 15 minutes of inactivity:

```
[org/gnome/desktop/screensaver]
idle-activation-enabled=true
```

Update the system databases:

```
# dconf update
```

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

Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

1.15 OL07-00-010101 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must prevent a user from overriding the screensaver idle-activation-enabled setting for the graphical user interface.

```
GROUP ID: V-221665
RULE ID: SV-221665r958402
```

Rationale:

A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence.

The session lock is implemented at the point where session activity can be determined.

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

Audit:

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

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

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

grep system-db /etc/dconf/profile/user

system-db:local

Check for the idle-activation-enabled setting with the following command:

Note: The example below is using the database "local" for the system, so the path is "/etc/dconf/db/local.d". This path must be modified if a database other than "local" is being used.

```
 # grep -i idle-activation-enabled /etc/dconf/db/local.d/locks/*
 /org/gnome/desktop/screensaver/idle-activation-enabled
```

If the command does not return a result, this is a finding.

Remediation:

Configure the operating system to prevent a user from overriding a screensaver lock after a 15-minute period of inactivity for graphical user interfaces.

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

Note: The example below is using the database "local" for the system, so if the system is using another database in "/etc/dconf/profile/user", the file should be created under the appropriate subdirectory.

```
# touch /etc/dconf/db/local.d/locks/session
```

Add the setting to lock the screensaver idle-activation-enabled setting:

```
/org/gnome/desktop/screensaver/idle-activation-enabled
```

Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

1.16 OL07-00-010110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must initiate a session lock for graphical user interfaces when the screensaver is activated.

```
GROUP ID: V-221666
RULE ID: SV-221666r958402
```

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 lock their operating system session manually prior to leaving the workstation, operating systems must be able to identify when a user's session has idled, and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled.

Audit:

Verify the operating system initiates a session lock a for graphical user interfaces when the screensaver is activated.

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

If GNOME is installed, check to see a session lock occurs when the screensaver is activated with the following command:

```
 # grep -i lock-delay /etc/dconf/db/local.d/*
 lock-delay=uint32 5
```

If the "lock-delay" setting is missing, or is not set to "5" or less, this is a finding.

Remediation:

Configure the operating system to initiate a session lock for graphical user interfaces when a screensaver is activated.

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

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

Add the setting to enable session locking when a screensaver is activated:

```
[org/gnome/desktop/screensaver]
lock-delay=uint32 5
```

The "uint32" must be included along with the integer key values as shown.

Update the system databases:

```
# dconf update
```

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

Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

1.17 OL07-00-010118 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that /etc/pam.d/passwd implements /etc/pam.d/system-auth when changing passwords.

```
GROUP ID: V-221667
RULE ID: SV-221667r1015164
```

Rationale:

Pluggable authentication modules (PAM) allow for a modular approach to integrating authentication methods. PAM operates in a top-down processing model and if the modules are not listed in the correct order, an important security function could be bypassed if stack entries are not centralized.

Audit:

Verify that /etc/pam.d/passwd is configured to use /etc/pam.d/system-auth when changing passwords:

```
# cat /etc/pam.d/passwd | grep -i substack | grep -i system-auth
password substack system-auth
```

If no results are returned, the line is commented out, this is a finding.

Remediation:

Configure PAM to utilize /etc/pam.d/system-auth when changing passwords.

Add the following line to "/etc/pam.d/passwd" (or modify the line to have the required value):

```
password substack system-auth
```

Additional Information:

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

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.18 OL07-00-010119 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that when passwords are changed or new passwords are established, pwquality must be used.

```
GROUP ID: V-221668
RULE ID: SV-221668r1015165
```

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.

Satisfied: SRG-OS-000480-GPOS-00229, SRG-OS-000069-GPOS-00037

Audit:

Verify the operating system uses "pwquality" to enforce the password complexity rules.

Check for the use of "pwquality" with the following command:

```
 # cat /etc/pam.d/system-auth | grep pam_pwquality

 password requisite pam_pwquality.so retry=3
```

If the command does not return an uncommented line containing the value "pam_pwquality.so" as shown, this is a finding.

If the value of "retry" is set to "0" or greater than "3", this is a finding.

Remediation:

Configure the operating system to use "pwquality" to enforce password complexity rules.

Add the following line to "/etc/pam.d/system-auth" (or modify the line to have the required value):

```
 password requisite pam_pwquality.so retry=3
```

Note: The value of "retry" should be between "1" and "3".

Additional Information:

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

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.19 OL07-00-010120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that when passwords are changed or new passwords are established, the new password must contain at least one upper-case character.

```
GROUP ID: V-221669
RULE ID: SV-221669r1015166
```

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 of several factors that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that must be tested before the password is compromised.

Audit:

Note: The value to require a number of upper-case characters to be set is expressed as a negative number in "/etc/security/pwquality.conf".

Check the value for "ucredit" in "/etc/security/pwquality.conf" with the following command:

```
# grep ucredit /etc/security/pwquality.conf
ucredit = -1
```

If the value of "ucredit" is not set to a negative value, this is a finding.

Remediation:

Configure the operating system to enforce password complexity by requiring that at least one upper-case character be used by setting the "ucredit" option.

Add the following line to "/etc/security/pwquality.conf" (or modify the line to have the required value):

```
ucredit = -1
```

Additional Information:

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

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.20 OL07-00-010130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that when passwords are changed or new passwords are established, the new password must contain at least one lower-case character.

```
GROUP ID: V-221670
RULE ID: SV-221670r1015167
```

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 of several factors that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that must be tested before the password is compromised.

Audit:

Note: The value to require a number of lower-case characters to be set is expressed as a negative number in "/etc/security/pwquality.conf".

Check the value for "lcredit" in "/etc/security/pwquality.conf" with the following command:

```
# grep lcredit /etc/security/pwquality.conf
lcredit = -1
```

If the value of "lcredit" is not set to a negative value, this is a finding.

Remediation:

Configure the system to require at least one lower-case character when creating or changing a password.

Add or modify the following line

in "/etc/security/pwquality.conf":

```
lcredit = -1
```

Additional Information:

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

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.21 OL07-00-010140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that when passwords are changed or new passwords are assigned, the new password must contain at least one numeric character.

```
GROUP ID: V-221671
RULE ID: SV-221671r1015168
```

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 of several factors that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that must be tested before the password is compromised.

Audit:

Note: The value to require a number of numeric characters to be set is expressed as a negative number in "/etc/security/pwquality.conf".

Check the value for "dcredit" in "/etc/security/pwquality.conf" with the following command:

```
# grep dcredit /etc/security/pwquality.conf
dcredit = -1
```

If the value of "dcredit" is not set to a negative value, this is a finding.

Remediation:

Configure the operating system to enforce password complexity by requiring that at least one numeric character be used by setting the "dcredit" option.

Add the following line to /etc/security/pwquality.conf (or modify the line to have the required value):

```
dcredit = -1
```

Additional Information:

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

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.22 OL07-00-010150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that when passwords are changed or new passwords are established, the new password must contain at least one special character.

```
GROUP ID: V-221672
RULE ID: SV-221672r1015169
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

Verify the operating system enforces password complexity by requiring that at least one special character be used.

Note: The value to require a number of special characters to be set is expressed as a negative number in "/etc/security/pwquality.conf".

Check the value for "ocredit" in "/etc/security/pwquality.conf" with the following command:

```
# grep ocredit /etc/security/pwquality.conf
ocredit=-1
```

If the value of "ocredit" is not set to a negative value, this is a finding.

Remediation:

Configure the operating system to enforce password complexity by requiring that at least one special character be used by setting the "ocredit" option.

Add the following line to "/etc/security/pwquality.conf" (or modify the line to have the required value):

```
ocredit = -1
```

Additional Information:

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

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.23 OL07-00-010160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that when passwords are changed a minimum of eight of the total number of characters must be changed.

```
GROUP ID: V-221673
RULE ID: SV-221673r1015170
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

The "difok" option sets the number of characters in a password that must not be present in the old password.

Check for the value of the "difok" option in "/etc/security/pwquality.conf" with the following command:

```
# grep difok /etc/security/pwquality.conf
difok = 8
```

If the value of "difok" is set to less than "8", this is a finding.

Remediation:

Configure the operating system to require the change of at least eight of the total number of characters when passwords are changed by setting the "difok" option.

Add the following line to "/etc/security/pwquality.conf" (or modify the line to have the required value):

```
difok = 8
```

Additional Information:

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

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.24 OL07-00-010170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that when passwords are changed a minimum of four character classes must be changed.

```
GROUP ID: V-221674
RULE ID: SV-221674r1015171
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

The "minclass" option sets the minimum number of required classes of characters for the new password (digits, uppercase, lower-case, others).

Check for the value of the "minclass" option in "/etc/security/pwquality.conf" with the following command:

```
# grep minclass /etc/security/pwquality.conf
minclass = 4
```

If the value of "minclass" is set to less than "4", this is a finding.

Remediation:

Configure the operating system to require the change of at least four character classes when passwords are changed by setting the "minclass" option.

Add the following line to "/etc/security/pwquality.conf conf" (or modify the line to have the required value):

```
minclass = 4
```

Additional Information:

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

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.25 OL07-00-010180 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that when passwords are changed the number of repeating consecutive characters must not be more than three characters.

```
GROUP ID: V-221675
RULE ID: SV-221675r1015172
```

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 of several factors that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

The "maxrepeat" option sets the maximum number of allowed same consecutive characters in a new password.

Check for the value of the "maxrepeat" option in "/etc/security/pwquality.conf" with the following command:

```
# grep maxrepeat /etc/security/pwquality.conf

maxrepeat = 3
```

If the value of "maxrepeat" is set to more than "3", this is a finding.

Remediation:

Configure the operating system to require the change of the number of repeating consecutive characters when passwords are changed by setting the "maxrepeat" option.

Add the following line to "/etc/security/pwquality.conf conf" (or modify the line to have the required value):

```
maxrepeat = 3
```

Additional Information:

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

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.26 OL07-00-010190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that when passwords are changed the number of repeating characters of the same character class must not be more than four characters.

```
GROUP ID: V-221676
RULE ID: SV-221676r1015173
```

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 of several factors that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

The "maxclassrepeat" option sets the maximum number of allowed same consecutive characters in the same class in the new password.

Check for the value of the "maxclassrepeat" option in "/etc/security/pwquality.conf" with the following command:

```
$ sudo grep maxclassrepeat /etc/security/pwquality.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 the operating system to require the change of the number of repeating characters of the same character class when passwords are changed by setting the "maxclassrepeat" option.

Add the following line to "/etc/security/pwquality.conf" conf (or modify the line to have the required value):

```
maxclassrepeat = 4
```

Additional Information:

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

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.27 OL07-00-010199 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured to prevent overwriting of custom authentication configuration settings by the authconfig utility.

```
GROUP ID: V-255902
RULE ID: SV-255902r1015197
```

Rationale:

When using the authconfig utility to modify authentication configuration settings, the "system-auth" and "password-auth" files and any custom settings that they may contain are overwritten. This can be avoided by creating new local configuration files and creating new or moving existing symbolic links to them. The authconfig utility will recognize the local configuration files and not overwrite them, while writing its own settings to the original configuration files.

Audit:

Verify "system-auth" and "password-auth" files are symbolic links pointing to "system-auth-local" and "password-auth-local":

```
$ sudo ls -l /etc/pam.d/{password,system}-auth

lrwxrwxrwx. 1 root root 30 Apr 1 11:59 /etc/pam.d/password-auth ->
/etc/pam.d/password-auth-local
lrwxrwxrwx. 1 root root 28 Apr 1 11:59 /etc/pam.d/system-auth ->
/etc/pam.d/system-auth-local
```

If system-auth and password-auth files are not symbolic links, this is a finding.

If system-auth and password-auth are symbolic links but do not point to "system-auth-local" and "password-auth-local", this is a finding.

Remediation:

Create custom configuration files and their corresponding symbolic links:

Rename the existing configuration files (skip this step if symbolic links are already present):

```
$ sudo mv /etc/pam.d/system-auth /etc/pam.d/system-auth-ac
$ sudo mv /etc/pam.d/password-auth /etc/pam.d/password-auth-ac
```

Create custom system-auth configuration file:

```
$ sudo vi /etc/pam.d/system-auth-local
```

The new file, at minimum, must contain the following lines:

```
auth        required      pam_faillock.so preauth silent audit deny=3
even_deny_root fail_interval=900 unlock_time=900
auth        include       system-auth-ac
auth        sufficient    pam_unix.so try_first_pass
auth        [default=die] pam_faillock.so authfail audit deny=3
even_deny_root fail_interval=900 unlock_time=900

account     required      pam_faillock.so
account     include       system-auth-ac

password    requisite     pam_pwhistory.so remember=5 retry=3
password    requisite     pam_pwquality.so retry=3
password    include       system-auth-ac
password    sufficient    pam_unix.so sha512 shadow try_first_pass
use_authtok

session     include       system-auth-ac
```

Create custom password-auth configuration file:

```
$ sudo vi /etc/pam.d/password-auth-local
```

The new file, at minimum, must contain the following lines:

```
auth        required      pam_faillock.so preauth silent audit deny=3
even_deny_root fail_interval=900 unlock_time=900
auth        include       password-auth-ac
auth        sufficient    pam_unix.so try_first_pass
auth        [default=die] pam_faillock.so authfail audit deny=3
even_deny_root fail_interval=900 unlock_time=900

account     required      pam_faillock.so
account     include       password-auth-ac

password    requisite     pam_pwhistory.so use_authtok remember=5 retry=3
password    requisite     pam_pwquality.so retry=3
password    include       password-auth-ac
password    sufficient    pam_unix.so sha512 shadow try_first_pass
use_authtok

session     include       password-auth-ac
```

Create new or move existing symbolic links to the new custom configuration files:

```
$ sudo ln -sf /etc/pam.d/system-auth-local /etc/pam.d/system-auth
$ sudo ln -sf /etc/pam.d/password-auth-local /etc/pam.d/password-auth
```

Once finished, the following file structure should be present:

```
$ sudo ls -1 /etc/pam.d/{password,system}-auth*

/etc/pam.d/password-auth
/etc/pam.d/password-auth-ac
/etc/pam.d/password-auth-local
/etc/pam.d/system-auth
/etc/pam.d/system-auth-ac
/etc/pam.d/system-auth-local
```

Note: With this solution in place, any custom settings to "system-auth" and "password-auth" will be retained and not overwritten by the use of the authconfig utility. The authconfig utility will write its settings to "system-auth-ac" and "password-auth-ac" and continue to function as expected.

Additional Information:

CCI-000196 The information system, for password-based authentication, stores only cryptographically-protected passwords.

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

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)

1.28 OL07-00-010200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that the PAM system service is configured to store only encrypted representations of passwords.

```
GROUP ID: V-221677
RULE ID: SV-221677r1015174
```

Rationale:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Audit:

Verify the PAM system service is configured to store only encrypted representations of passwords. The strength of encryption that must be used to hash passwords for all accounts is SHA512.

Check that the system is configured to create SHA512 hashed passwords with the following command:

```
# grep password /etc/pam.d/system-auth /etc/pam.d/password-auth
```

Outcome should look like following:

```
/etc/pam.d/system-auth-ac:password sufficient pam_unix.so sha512 shadow
try_first_pass use_authtok
/etc/pam.d/password-auth:password sufficient pam_unix.so sha512 shadow
try_first_pass use_authtok
```

If the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" configuration files allow for password hashes other than SHA512 to be used, this is a finding.

Remediation:

Configure the operating system to store only SHA512 encrypted representations of passwords.

Add the following line in "/etc/pam.d/system-auth":

```
password    sufficient    pam_unix.so sha512 shadow try_first_pass
use_authtok
```

Add the following line in "/etc/pam.d/password-auth":

```
password    sufficient    pam_unix.so sha512 shadow try_first_pass
use_authtok
```

Note: Per requirement OL07-00-010199, Oracle Linux 7 must be configured to not overwrite custom authentication configuration settings while using the authconfig utility; otherwise, manual changes to the listed files will be overwritten whenever the authconfig utility is used.

Additional Information:

CCI-000196 The information system, for password-based authentication, stores only cryptographically-protected passwords.

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

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)

1.29 OL07-00-010210 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured to use the shadow file to store only encrypted representations of passwords.

```
GROUP ID: V-221678
RULE ID: SV-221678r1015175
```

Rationale:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Audit:

Verify the system's shadow file is configured to store only encrypted representations of passwords. The strength of encryption that must be used to hash passwords for all accounts is SHA512.

Check that the system is configured to create SHA512 hashed passwords with the following command:

```
# grep -i encrypt /etc/login.defs
ENCRYPT_METHOD SHA512
```

If the "/etc/login.defs" configuration file does not exist or allows for password hashes other than SHA512 to be used, this is a finding.

Remediation:

Configure the operating system to store only SHA512 encrypted representations of passwords.

Add or update the following line in "/etc/login.defs":

```
ENCRYPT_METHOD SHA512
```

Additional Information:

CCI-000196 The information system, for password-based authentication, stores only cryptographically-protected passwords.

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

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)

1.30 OL07-00-010220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that user and group account administration utilities are configured to store only encrypted representations of passwords.

```
GROUP ID: V-221680
RULE ID: SV-221680r1015176
```

Rationale:

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised. Passwords encrypted with a weak algorithm are no more protected than if they are kept in plain text.

Audit:

Verify the user and group account administration utilities are configured to store only encrypted representations of passwords. The strength of encryption that must be used to hash passwords for all accounts is "SHA512".

Check that the system is configured to create "SHA512" hashed passwords with the following command:

```
# grep -i sha512 /etc/libuser.conf

crypt_style = sha512
```

If the "crypt_style" variable is not set to "sha512", is not in the defaults section, is commented out, or does not exist, this is a finding.

Remediation:

Configure the operating system to store only SHA512 encrypted representations of passwords.

Add or update the following line in "/etc/libuser.conf" in the [defaults] section:

```
crypt_style = sha512
```

Additional Information:

CCI-000196 The information system, for password-based authentication, stores only cryptographically-protected passwords.

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

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)

1.31 OL07-00-010230 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that passwords for new users are restricted to a 24 hours/1 day minimum lifetime.

```
GROUP ID: V-221681
RULE ID: SV-221681r1015177
```

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 the operating system enforces 24 hours/1 day 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 the operating system to enforce 24 hours/1 day 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-000198 The information system enforces minimum password lifetime restrictions.

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

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.32 OL07-00-010250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that passwords for new users are restricted to a 60-day maximum lifetime.

```
GROUP ID: V-221683
RULE ID: SV-221683r1038967
```

Rationale:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Audit:

If passwords are not being used for authentication, this is Not Applicable.

Verify the operating system enforces a 60-day maximum password lifetime restriction for new user accounts.

Check for the value of "PASS_MAX_DAYS" in "/etc/login.defs" with the following command:

```
# grep -i pass_max_days /etc/login.defs
PASS_MAX_DAYS 60
```

If the "PASS_MAX_DAYS" parameter value is not 60 or less, or is commented out, this is a finding.

Remediation:

Configure the operating system to enforce a 60-day maximum password lifetime restriction.

Add the following line in "/etc/login.defs" (or modify the line to have the required value):

```
PASS_MAX_DAYS 60
```

Additional Information:

CCI-000199 The information system enforces maximum password lifetime restrictions.

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

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.33 OL07-00-010240 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that passwords are restricted to a 24 hours/1 day minimum lifetime.

```
GROUP ID: V-221682
RULE ID: SV-221682r1015178
```

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:

Check whether the minimum time period between password changes for each user account is one day or greater.

```
# awk -F: '$4 < 1 {print $1 " " $4}' /etc/shadow
```

If any results are returned that are not associated with a system account, this is a finding.

Remediation:

Configure non-compliant accounts to enforce a 24 hours/1 day minimum password lifetime:

```
# chage -m 1 [user]
```

Additional Information:

CCI-000198 The information system enforces minimum password lifetime restrictions.

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

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.34 OL07-00-010260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that existing passwords are restricted to a 60-day maximum lifetime.

```
GROUP ID: V-221684
RULE ID: SV-221684r1038967
```

Rationale:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords need to be changed periodically. If the operating system does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the operating system passwords could be compromised.

Audit:

Check whether the maximum time period for existing passwords is restricted to 60 days.

```
# awk -F: '$5 > 60 {print $1 " " $5}' /etc/shadow
```

If any results are returned that are not associated with a system account, this is a finding.

Remediation:

Configure non-compliant accounts to enforce a 60-day maximum password lifetime restriction.

```
# chage -M 60 [user]
```

Additional Information:

CCI-000199 The information system enforces maximum password lifetime restrictions.

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

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.35 OL07-00-010271 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must automatically expire temporary accounts within 72 hours.

```
GROUP ID: V-254522
RULE ID: SV-254522r958508
```

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.

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-001682 Automatically remove or disable emergency accounts after an organization-defined time period for each type of account.

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

1.36 OL07-00-010280 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that passwords are a minimum of 15 characters in length.

```
GROUP ID: V-221686
RULE ID: SV-221686r1015181
```

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.

Audit:

Verify the operating system enforces a minimum 15-character password length. The "minlen" option sets the minimum number of characters in a new password.

Check for the value of the "minlen" option in "/etc/security/pwquality.conf" with the following command:

```
# grep minlen /etc/security/pwquality.conf
minlen = 15
```

If the command does not return a "minlen" value of 15 or greater, this is a finding.

Remediation:

Configure operating system to enforce a minimum 15-character password length.

Add the following line to "/etc/security/pwquality.conf" (or modify the line to have the required value):

```
minlen = 15
```

Additional Information:

CCI-000205 The information system enforces minimum password length.

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

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.37 OL07-00-010290 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must not allow accounts configured with blank or null passwords.

```
GROUP ID: V-221687
RULE ID: SV-221687r991589
```

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.

Audit:

To verify that null passwords cannot be used, run the following command:

```
 # grep nullok /etc/pam.d/system-auth /etc/pam.d/password-auth
```

If this produces any output, it may be possible to log on with accounts with empty passwords.

If null passwords can be used, this is a finding.

Remediation:

If an account is configured for password authentication but does not have an assigned password, it may be possible to log on to the account without authenticating.

Remove any instances of the "nullok" option in "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" to prevent logons with empty passwords.

Note: Per requirement OL07-00-010199, Oracle Linux 7 must be configured to not overwrite custom authentication configuration settings while using the authconfig utility, otherwise manual changes to the listed files will be overwritten whenever the authconfig utility is used.

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.38 OL07-00-010291 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must not have accounts configured with blank or null passwords.

```
GROUP ID: V-251698
RULE ID: SV-251698r991589
```

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 must never be used in operational environments.

Audit:

Check the "/etc/shadow" file for blank passwords 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 the system to have a password or lock the account with the following commands:

Perform a password reset:

```
$ sudo passwd [username]
```

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

1.39 OL07-00-010300 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must be configured so that the SSH daemon does not allow authentication using an empty password.

```
GROUP ID: V-221688
RULE ID: SV-221688r958486
```

Rationale:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Audit:

To determine how the SSH daemon's "PermitEmptyPasswords" option is set, run the following command:

```
# grep -i PermitEmptyPasswords /etc/ssh/sshd_config
PermitEmptyPasswords no
```

If no line, a commented line, or a line indicating the value "no" is returned, the required value is set.

If the required value is not set, this is a finding.

Remediation:

To explicitly disallow remote logon from accounts with empty passwords, add or correct the following line in "/etc/ssh/sshd_config":

```
PermitEmptyPasswords no
```

The SSH service must be restarted for changes to take effect. Any accounts with empty passwords should be disabled immediately, and PAM configuration should prevent users from being able to assign themselves empty passwords.

Additional Information:

CCI-000766 Implement multifactor authentication for access to non-privileged accounts.

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

1.40 OL07-00-010310 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must disable account identifiers (individuals, groups, roles, and devices) if the password expires.

```
GROUP ID: V-221689
RULE ID: SV-221689r1015184
```

Rationale:

Inactive identifiers pose a risk to systems and applications because attackers may exploit an inactive identifier and potentially obtain undetected access to the system. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained.

Operating systems need to track periods of inactivity and disable application identifiers after 35 days of inactivity.

Audit:

If passwords are not being used for authentication, this is Not Applicable.

Verify the operating system disables account identifiers (individuals, groups, roles, and devices) after the password has expired with the following command:

```
 # grep -i inactive /etc/default/useradd
 INACTIVE=35
```

If "INACTIVE" is set to "-1", a value greater than "35", is commented out, or is not defined, this is a finding.

Remediation:

Configure the operating system to disable account identifiers (individuals, groups, roles, and devices) 35 days after the password has expired.

Add the following line to "/etc/default/useradd" (or modify the line to have the required value):

```
 INACTIVE=35
```

DOD recommendation is 35 days, but a lower value is acceptable. The value "-1" will disable this feature, and "0" will disable the account immediately after the password expires.

Additional Information:

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 800-53A::IA-4.1 (iii)
- NIST SP 800-53 Revision 4::IA-4 e

CCI-003627 Disable accounts when the accounts have expired.

- NIST SP 800-53 Revision 5::AC-2 (3) (a)

1.41 OL07-00-010320 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured to lock accounts for a minimum of 15 minutes after three unsuccessful logon attempts within a 15-minute timeframe.

```
GROUP ID: V-221690
RULE ID: SV-221690r958388
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005

Audit:

Check that the system locks an account for a minimum of 15 minutes after three unsuccessful logon attempts within a period of 15 minutes with the following command:

```
# grep pam_faillock.so /etc/pam.d/password-auth

auth        required      pam_faillock.so preauth silent audit deny=3
even_deny_root fail_interval=900 unlock_time=900
auth        [default=die] pam_faillock.so authfail audit deny=3
even_deny_root fail_interval=900 unlock_time=900
account     required      pam_faillock.so
```

If the "deny" parameter is set to "0" or a value greater than "3" on both "auth" lines with the "pam_faillock.so" module, or is missing from these lines, this is a finding.

If the "even_deny_root" parameter is not set on both "auth" lines with the "pam_faillock.so" module, or is missing from these lines, this is a finding.

If the "fail_interval" parameter is set to "0" or is set to a value less than "900" on both "auth" lines with the "pam_faillock.so" module, or is missing from these lines, this is a finding.

If the "unlock_time" parameter is not set to "0", "never", or is set to a value less than "900" on both "auth" lines with the "pam_faillock.so" module, or is missing from these lines, this is a finding.

Note: The maximum configurable value for "unlock_time" is "604800".

If any line referencing the "pam_faillock.so" module is commented out, this is a finding.

```
# grep pam_faillock.so /etc/pam.d/system-auth

auth        required      pam_faillock.so preauth silent audit deny=3
even_deny_root fail_interval=900 unlock_time=900
auth        [default=die] pam_faillock.so authfail audit deny=3
even_deny_root fail_interval=900 unlock_time=900
account     required      pam_faillock.so
```

If the "deny" parameter is set to "0" or a value greater than "3" on both "auth" lines with the "pam_faillock.so" module, or is missing from these lines, this is a finding.

If the "even_deny_root" parameter is not set on both "auth" lines with the "pam_faillock.so" module, or is missing from these lines, this is a finding.

If the "fail_interval" parameter is set to "0" or is set to a value less than "900" on both "auth" lines with the "pam_faillock.so" module, or is missing from these lines, this is a finding.

If the "unlock_time" parameter is not set to "0", "never", or is set to a value less than "900" on both "auth" lines with the "pam_faillock.so" module or is missing from these lines, this is a finding.

Note: The maximum configurable value for "unlock_time" is "604800".

If any line referencing the "pam_faillock.so" module is commented out, this is a finding.

Remediation:

Configure the operating system to lock an account for the maximum period when three unsuccessful logon attempts in 15 minutes are made.

Add/Modify the appropriate sections of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

```
auth        required      pam_faillock.so preauth silent audit deny=3
even_deny_root fail_interval=900 unlock_time=900
auth        sufficient    pam_unix.so try_first_pass
auth        [default=die] pam_faillock.so authfail audit deny=3
even_deny_root fail_interval=900 unlock_time=900
account     required      pam_faillock.so
```

Note: Per requirement OL07-00-010199, Oracle Linux 7 must be configured to not overwrite custom authentication configuration settings while using the authconfig utility, otherwise manual changes to the listed files will be overwritten whenever the authconfig utility is used.

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

CCI-002236 Defines the time period the information system will automatically lock the account or node 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

CCI-002237 Defines the delay algorithm to delay the next logon prompt 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

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

1.42 OL07-00-010330 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must lock the associated account after three unsuccessful root logon attempts are made within a 15-minute period.

```
GROUP ID: V-221691
RULE ID: SV-221691r958736
```

Rationale:

By limiting the number of failed logon attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-OS-000329-GPOS-00128, SRG-OS-000021-GPOS-00005

Audit:

Verify the operating system automatically locks the root account, for a minimum of 15 minutes, when three unsuccessful logon attempts in 15 minutes are made.

```
# grep pam_faillock.so /etc/pam.d/password-auth

auth        required      pam_faillock.so preauth silent audit deny=3
even_deny_root fail_interval=900 unlock_time=900
auth        [default=die] pam_faillock.so authfail audit deny=3
even_deny_root fail_interval=900 unlock_time=900
account     required      pam_faillock.so
```

If the "even_deny_root" setting is not defined on both lines with the "pam_faillock.so" module, is commented out, or is missing from a line, this is a finding.

```
# grep pam_faillock.so /etc/pam.d/system-auth

auth        required      pam_faillock.so preauth silent audit deny=3
even_deny_root fail_interval=900 unlock_time=900
auth        [default=die] pam_faillock.so authfail audit deny=3
even_deny_root fail_interval=900 unlock_time=900
account     required      pam_faillock.so
```

If the "even_deny_root" setting is not defined on both lines with the "pam_faillock.so" module, is commented out, or is missing from a line, this is a finding.

Remediation:

Configure the operating system to automatically lock the root account, for a minimum of 15 minutes, when three unsuccessful logon attempts in 15 minutes are made.

Modify the first three lines of the auth section and the first line of the account section of the "/etc/pam.d/system-auth" and "/etc/pam.d/password-auth" files to match the following lines:

```
auth        required      pam_faillock.so preauth silent audit deny=3
even_deny_root fail_interval=900 unlock_time=900
auth        sufficient    pam_unix.so try_first_pass
auth        [default=die] pam_faillock.so authfail audit deny=3
even_deny_root fail_interval=900 unlock_time=900
account     required      pam_faillock.so
```

Note: Per requirement OL07-00-010199, Oracle Linux 7 must be configured to not overwrite custom authentication configuration settings while using the authconfig utility, otherwise manual changes to the listed files will be overwritten whenever the authconfig utility is used.

Additional Information:

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

1.43 OL07-00-010339 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must specify the default "include" directory for the /etc/sudoers file.

```
GROUP ID: V-251699
RULE ID: SV-251699r991589
```

Rationale:

The "sudo" command allows authorized users to run programs (including shells) as other users, system users, and root. The "/etc/sudoers" file is used to configure authorized "sudo" users as well as the programs they are allowed to run. Some configuration options in the "/etc/sudoers" file allow configured users to run programs without re-authenticating. Use of these configuration options makes it easier for one compromised account to be used to compromise other accounts.

It is possible to include other sudoers files from within the sudoers file currently being parsed using the #include and #includedir directives. When sudo reaches this line it will suspend processing of the current file (/etc/sudoers) and switch to the specified file/directory. Once the end of the included file(s) is reached, the rest of /etc/sudoers will be processed. Files that are included may themselves include other files. A hard limit of 128 nested include files is enforced to prevent include file loops.

Audit:

Note: If the "include" and "includedir" directives are not present in the /etc/sudoers file, this requirement is not applicable.

Verify the operating system specifies only the default "include" directory for the /etc/sudoers file with the following command:

```
$ sudo grep include /etc/sudoers
#includedir /etc/sudoers.d
```

If the results are not "/etc/sudoers.d" or additional files or directories are specified, this is a finding.

Verify the operating system does not have nested "include" files or directories within the /etc/sudoers.d directory with the following command:

```
$ sudo grep -r include /etc/sudoers.d
```

If results are returned, this is a finding.

Remediation:

Configure the /etc/sudoers file to only include the /etc/sudoers.d directory.

Edit the /etc/sudoers file with the following command:

```
$ sudo visudo
```

Add or modify the following line:

```
#includedir /etc/sudoers.d
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.44 OL07-00-010340 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that users must provide a password for privilege escalation.

```
GROUP ID: V-221692
RULE ID: SV-221692r1050789
```

Rationale:

Without reauthentication, users may access resources or perform tasks for which authorization has not been granted.

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 requires users to supply a password for privilege escalation.

Check the configuration of the "/etc/sudoers" and "/etc/sudoers.d/*" files with the following command:

```
$ sudo grep -ir 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 utilizing MFA, this is a finding.

Remediation:

Configure the operating system to require users to supply a password for privilege escalation.

Check the configuration of the "/etc/sudoers" file with the following command:

```
$ sudo visudo
```

Remove any occurrences of "NOPASSWD" tags in the file.

Check the configuration of the /etc/sudoers.d/* files with the following command:

```
$ sudo grep -ir nopasswd /etc/sudoers.d
```

Remove any occurrences of "NOPASSWD" tags in the file.

Additional Information:

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4::IA-11
- NIST SP 800-53 Revision 5::IA-11

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

1.45 OL07-00-010341 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must restrict privilege elevation to authorized personnel.

```
GROUP ID: V-237627
RULE ID: SV-237627r991589
```

Rationale:

The sudo command allows a user to execute programs with elevated (administrator) privileges. It prompts the user for their password and confirms your request to execute a command by checking a file, called sudoers. If the "sudoers" file is not configured correctly, any user defined on the system can initiate privileged actions on the target system.

Audit:

Verify the "sudoers" file restricts sudo access to authorized personnel.

```
$ sudo grep -iw 'ALL' /etc/sudoers /etc/sudoers.d/*
```

If the either of the following entries are returned, this is a finding:

```
ALL     ALL=(ALL) ALL
ALL     ALL=(ALL:ALL) ALL
```

Remediation:

Remove the following entries from the sudoers file:

```
ALL     ALL=(ALL) ALL
ALL     ALL=(ALL:ALL) ALL
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.46 OL07-00-010342 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must use the invoking user's password for privilege escalation when using "sudo".

```
GROUP ID: V-237628
RULE ID: SV-237628r991589
```

Rationale:

The sudoers security policy requires that users authenticate themselves before they can use sudo. When sudoers requires authentication, it validates the invoking user's credentials. If the rootpw, targetpw, or runaspw flags are defined and not disabled, by default the operating system will prompt the invoking user for the "root" user password. For more information on each of the listed configurations, reference the sudoers(5) manual page.

Audit:

Verify that the sudoers security policy is configured to use the invoking user's password for privilege escalation.

```
$ sudo grep -Eir '(rootpw|targetpw|runaspw)' /etc/sudoers /etc/sudoers.d* |
grep -v '#'

/etc/sudoers:Defaults !targetpw
/etc/sudoers:Defaults !rootpw
/etc/sudoers:Defaults !runaspw
```

If conflicting results are returned, this is a finding.

If "Defaults !targetpw" is not defined, this is a finding.

If "Defaults !rootpw" is not defined, this is a finding.

If "Defaults !runaspw" is not defined, this is a finding.

Remediation:

Define the following in the Defaults section of the /etc/sudoers file or a configuration file in the /etc/sudoers.d/ directory:

```
Defaults !targetpw
Defaults !rootpw
Defaults !runaspw
```

Remove any configurations that conflict with the above from the following locations:

```
/etc/sudoers
/etc/sudoers.d/
```

Additional Information:

CCI-002227 Restrict privileged accounts on the system to organization-defined personnel or roles.

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

1.47 OL07-00-010343 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must require re-authentication when using the "sudo" command.

```
GROUP ID: V-237629
RULE ID: SV-237629r1050789
```

Rationale:

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the organization requires the user to re-authenticate when using the "sudo" command.

If the value is set to an integer less than 0, the user's time stamp will not expire and the user will not have to re-authenticate for privileged actions until the user's session is terminated.

Audit:

Verify the operating system requires re-authentication when using the "sudo" command to elevate privileges.

```
$ sudo grep -ir 'timestamp_timeout' /etc/sudoers /etc/sudoers.d

/etc/sudoers:Defaults timestamp_timeout=0
```

If conflicting results are returned, 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 the "sudo" command to require re-authentication.

Edit the /etc/sudoers file:

```
$ sudo visudo
```

Add or modify the following line:

```
Defaults timestamp_timeout=[value]
```

Note: The "[value]" must be a number that is greater than or equal to "0".

Remove any duplicate or conflicting lines from /etc/sudoers and /etc/sudoers.d/ files.

Additional Information:

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4::IA-11
- NIST SP 800-53 Revision 5::IA-11

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

1.48 OL07-00-010344 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must not be configured to bypass password requirements for privilege escalation.

```
GROUP ID: V-251700
RULE ID: SV-251700r1050789
```

Rationale:

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user re-authenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Audit:

Verify the operating system is not be configured to bypass password requirements for privilege escalation.

Check the configuration of the "/etc/pam.d/sudo" file with the following command:

```
$ sudo grep pam_succeed_if /etc/pam.d/sudo
```

If any occurrences of "pam_succeed_if" is returned from the command, this is a finding.

Remediation:

Configure the operating system to require users to supply a password for privilege escalation.

Check the configuration of the "/etc/ pam.d/sudo" file with the following command:

```
$ sudo vi /etc/pam.d/sudo
```

Remove any occurrences of "pam_succeed_if" in the file.

Additional Information:

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4::IA-11
- NIST SP 800-53 Revision 5::IA-11

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

1.49 OL07-00-010350 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so users must re-authenticate for privilege escalation.

```
GROUP ID: V-228569
RULE ID: SV-228569r1050789
```

Rationale:

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user reauthenticate.

Satisfies: SRG-OS-000373-GPOS-00156, SRG-OS-000373-GPOS-00157, SRG-OS-000373-GPOS-00158

Audit:

Verify the operating system requires users to reauthenticate for privilege escalation.

Check the configuration of the "/etc/sudoers" and "/etc/sudoers.d/*" files with the following command:

```
# grep -i authenticate /etc/sudoers /etc/sudoers.d/*
```

If any uncommented line is found with a "!authenticate" tag, this is a finding.

Remediation:

Configure the operating system to require users to reauthenticate for privilege escalation.

Check the configuration of the "/etc/sudoers" file with the following command:

```
# visudo
```

Remove any occurrences of "!authenticate" tags in the file.

Check the configuration of the "/etc/sudoers.d/*" files with the following command:

```
# grep -i authenticate /etc/sudoers /etc/sudoers.d/*
```

Remove any occurrences of "!authenticate" tags in the file(s).

Additional Information:

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4::IA-11
- NIST SP 800-53 Revision 5::IA-11

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

1.50 OL07-00-010375 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Oracle Linux operating system must restrict access to the kernel message buffer.

```
GROUP ID: V-255901
RULE ID: SV-255901r958524
```

Rationale:

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

Audit:

Verify the operating system is configured to restrict access to the kernel message buffer with the following commands:

```
$ 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 grep -r kernel.dmesg_restrict /run/sysctl.d/* /etc/sysctl.d/*
/usr/local/lib/sysctl.d/* /usr/lib/sysctl.d/* /lib/sysctl.d/*
/etc/sysctl.conf 2> /dev/null
/etc/sysctl.conf:kernel.dmesg_restrict = 1
/etc/sysctl.d/99-sysctl.conf:kernel.dmesg_restrict = 1
```

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

If conflicting results are returned, this is a finding.

Remediation:

Configure the operating system to restrict access to the kernel message buffer.

Set the system to the required kernel parameter by adding or modifying the following line in /etc/sysctl.conf or a config file in the /etc/sysctl.d/ directory:

```
kernel.dmesg_restrict = 1
```

Remove any configurations that conflict with the above from the following locations:

```
/run/sysctl.d/
/etc/sysctl.d/
/usr/local/lib/sysctl.d/
/usr/lib/sysctl.d/
/lib/sysctl.d/
/etc/sysctl.conf
```

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

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

Additional Information:

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

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

1.51 OL07-00-010430 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that the delay between logon prompts following a failed console logon attempt is at least four seconds.

```
GROUP ID: V-221693
RULE ID: SV-221693r991588
```

Rationale:

Configuring the operating system to implement organization-wide security implementation guides and security checklists verifies compliance with federal standards and establishes a common security baseline across DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture and/or functionality of the system. Security-related parameters are those parameters impacting the security state of the system, including the parameters required to satisfy other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory permission settings; and settings for functions, ports, protocols, services, and remote connections.

Audit:

Verify the operating system enforces a delay of at least four seconds between console logon prompts following a failed logon attempt.

Check the value of the "fail_delay" parameter in the "/etc/login.defs" file with the following command:

```
# grep -i fail_delay /etc/login.defs
FAIL_DELAY 4
```

If the value of "FAIL_DELAY" is not set to "4" or greater, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to enforce a delay of at least four seconds between logon prompts following a failed console logon attempt.

Modify the "/etc/login.defs" file to set the "FAIL_DELAY" parameter to "4" or greater:

```
FAIL_DELAY 4
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.52 OL07-00-010440 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must not allow an unattended or automatic logon to the system via a graphical user interface.

```
GROUP ID: V-221694
RULE ID: SV-221694r991591
```

Rationale:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Audit:

Verify the operating system does not allow an unattended or automatic logon to the system via a graphical user interface.

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

Check for the value of the "AutomaticLoginEnable" in the "/etc/gdm/custom.conf" file with the following command:

```
# grep -i automaticloginenable /etc/gdm/custom.conf
AutomaticLoginEnable=false
```

If the value of "AutomaticLoginEnable" is not set to "false", this is a finding.

Remediation:

Configure the operating system not to allow an unattended or automatic logon to the system via a graphical user interface.

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

Add or edit the line for the "AutomaticLoginEnable" parameter in the [daemon] section of the "/etc/gdm/custom.conf" file to "false":

```
[daemon]
AutomaticLoginEnable=false
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.53 OL07-00-010450 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must not allow an unrestricted logon to the system.

```
GROUP ID: V-221695
RULE ID: SV-221695r991591
```

Rationale:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Audit:

Verify the operating system does not allow an unrestricted logon to the system via a graphical user interface.

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

Check for the value of the "TimedLoginEnable" parameter in "/etc/gdm/custom.conf" file with the following command:

```
# grep -i timedloginenable /etc/gdm/custom.conf
TimedLoginEnable=false
```

If the value of "TimedLoginEnable" is not set to "false", this is a finding.

Remediation:

Configure the operating system not to allow an unrestricted account to log on to the system via a graphical user interface.

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

Add or edit the line for the "TimedLoginEnable" parameter in the [daemon] section of the "/etc/gdm/custom.conf" file to "false":

```
[daemon]
TimedLoginEnable=false
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.54 OL07-00-010460 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must not allow users to override SSH environment variables.

```
GROUP ID: V-221696
RULE ID: SV-221696r991591
```

Rationale:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Audit:

Verify the operating system does not allow users to override environment variables to the SSH daemon.

Check for the value of the "PermitUserEnvironment" keyword with the following command:

```
# grep -i permituserenvironment /etc/ssh/sshd_config
PermitUserEnvironment no
```

If the "PermitUserEnvironment" keyword is not set to "no", is missing, or is commented out, this is a finding.

Remediation:

Configure the operating system not to allow users to override environment variables to the SSH daemon.

Edit the "/etc/ssh/sshd_config" file to uncomment or add the line for "PermitUserEnvironment" keyword and set the value to "no":

```
PermitUserEnvironment no
```

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

1.55 OL07-00-010470 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must not allow a non-certificate trusted host SSH logon to the system.

```
GROUP ID: V-221697
RULE ID: SV-221697r991591
```

Rationale:

Failure to restrict system access to authenticated users negatively impacts operating system security.

Audit:

Verify the operating system does not allow a non-certificate trusted host SSH logon to the system.

Check for the value of the "HostbasedAuthentication" keyword with the following command:

```
# grep -i hostbasedauthentication /etc/ssh/sshd_config
HostbasedAuthentication no
```

If the "HostbasedAuthentication" keyword is not set to "no", is missing, or is commented out, this is a finding.

Remediation:

Configure the operating system not to allow a non-certificate trusted host SSH logon to the system.

Edit the "/etc/ssh/sshd_config" file to uncomment or add the line for "HostbasedAuthentication" keyword and set the value to "no":

```
HostbasedAuthentication no
```

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

1.56 OL07-00-010481 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must require authentication upon booting into single-user and maintenance modes.

```
GROUP ID: V-221699
RULE ID: SV-221699r958472
```

Rationale:

If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system.

Audit:

Verify the operating system must require authentication upon booting into single-user and maintenance modes.

Check that the operating system requires authentication upon booting into single-user mode with the following command:

```
# grep -i execstart /usr/lib/systemd/system/rescue.service | grep -i sulogin

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

If "ExecStart" does not have "/usr/sbin/sulogin" as an option, this is a finding.

Remediation:

Configure the operating system to require authentication upon booting into single-user and maintenance modes.

Add or modify the "ExecStart" line in "/usr/lib/systemd/system/rescue.service" to include "/usr/sbin/sulogin":

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

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

1.57 OL07-00-010482 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Oracle Linux operating systems version 7.2 or newer with a Basic Input/Output System (BIOS) must require authentication upon booting into single-user and maintenance modes.

```
GROUP ID: V-221700
RULE ID: SV-221700r958472
```

Rationale:

If the system does not require valid authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for Oracle Linux 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Audit:

For systems that use UEFI, this is Not Applicable.

For systems that are running a version of Oracle Linux prior to 7.2, this is Not Applicable.

Check to see if an encrypted grub superusers password is set. On systems that use BIOS, use the following command:

```
$ sudo grep -iw grub2_password /boot/grub2/user.cfg

GRUB2_PASSWORD=grub.pbkdf2.sha512.[password_hash]
```

If the grub superusers password does not begin with "grub.pbkdf2.sha512", this is a finding.

Remediation:

Configure the system to encrypt the boot password for the grub superusers account with the grub2-setpassword command, which creates/overwrites the /boot/grub2/user.cfg file.

Generate an encrypted grub2 password for the grub superusers account with the following command:

```
$ sudo grub2-setpassword

Enter password:
Confirm password:
```

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

1.58 OL07-00-010483 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Oracle Linux operating systems version 7.2 or newer booted with a BIOS must have a unique name for the grub superusers account when booting into single-user and maintenance modes.

```
GROUP ID: V-244555
RULE ID: SV-244555r958472
```

Rationale:

If the system does not require valid authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for Oracle Linux 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu. The GRUB 2 superuser account is an account of last resort. Establishing a unique username for this account hardens the boot loader against brute force attacks. Due to the nature of the superuser account database being distinct from the OS account database, this allows the use of a username that is not among those within the OS account database. Examples of non-unique superusers names are root, superuser, unlock, etc.

Audit:

For systems that use UEFI, this is Not Applicable.

For systems that are running a version of Oracle Linux prior to 7.2, this is Not Applicable.

Verify that a unique name is set as the "superusers" account:

```
$ sudo grep -iw "superusers" /boot/grub2/grub.cfg

set superusers="[someuniquestringhere]"
export superusers
```

If "superusers" is identical to any OS account name or is missing a name, this is a finding.

Remediation:

Configure the system to have a unique name for the grub superusers account.

Edit the /etc/grub.d/01_users file and add or modify the following lines:

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

Generate a new grub.cfg file with the following command:

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

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

1.59 OL07-00-010491 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Oracle Linux operating systems version 7.2 or newer using Unified Extensible Firmware Interface (UEFI) must require authentication upon booting into single-user and maintenance modes.

```
GROUP ID: V-221702
RULE ID: SV-221702r958472
```

Rationale:

If the system does not require valid authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for Oracle Linux 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu.

Audit:

For systems that use BIOS, this is Not Applicable.

For systems that are running a version of Oracle Linux prior to 7.2, this is Not Applicable.

Check to see if an encrypted grub superusers password is set. On systems that use UEFI, use the following command:

```
$ sudo grep -iw grub2_password /boot/efi/EFI/redhat/user.cfg

GRUB2_PASSWORD=grub.pbkdf2.sha512.[password_hash]
```

If the grub superusers password does not begin with "grub.pbkdf2.sha512", this is a finding.

Remediation:

Configure the system to encrypt the boot password for the grub superusers account with the grub2-setpassword command, which creates/overwrites the /boot/efi/EFI/redhat/user.cfg file.

Generate an encrypted grub2 password for the grub superusers account with the following command:

```
$ sudo grub2-setpassword

Enter password:
Confirm password:
```

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

1.60 OL07-00-010492 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Oracle Linux operating systems version 7.2 or newer booted with United Extensible Firmware Interface (UEFI) must have a unique name for the grub superusers account when booting into single-user mode and maintenance.

```
GROUP ID: V-244556
RULE ID: SV-244556r958472
```

Rationale:

If the system does not require valid authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system. GRUB 2 is the default boot loader for Oracle Linux 7 and is designed to require a password to boot into single-user mode or make modifications to the boot menu. The GRUB 2 superuser account is an account of last resort. Establishing a unique username for this account hardens the boot loader against brute force attacks. Due to the nature of the superuser account database being distinct from the OS account database, this allows the use of a username that is not among those within the OS account database. Examples of non-unique superusers names are root, superuser, unlock, etc.

Audit:

For systems that use BIOS, this is Not Applicable.

For systems that are running a version of Oracle Linux prior to 7.2, this is Not Applicable.

Verify that a unique name is set as the "superusers" account:

```
$ sudo grep -iw "superusers" /boot/efi/EFI/redhat/grub.cfg

set superusers="[someuniquestringhere]"
export superusers
```

If "superusers" is identical to any OS account name or is missing a name, this is a finding.

Remediation:

Configure the system to require a grub bootloader password for the grub superusers account.

Edit the /etc/grub.d/01_users file and add or modify the following lines:

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

Generate a new grub.cfg file with the following command:

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

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

1.61 OL07-00-010500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must uniquely identify and must authenticate organizational users (or processes acting on behalf of organizational users) using multifactor authentication.

```
GROUP ID: V-221703
RULE ID: SV-221703r1015186
```

Rationale:

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

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and processes acting on behalf of users) must be uniquely identified and authenticated to all accesses, except for the following:

1. Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication;

and

2. Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

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-000108-GPOS-00057, SRG-OS-000108-GPOS-00058

Audit:

Verify the operating system requires multifactor authentication to uniquely identify organizational users using multifactor authentication.

Check to see if smartcard authentication is enforced on the system:

```
# authconfig --test | grep "pam_pkcs11 is enabled"
```

If no results are returned, this is a finding.

```
# authconfig --test | grep "smartcard removal action"
```

If "smartcard removal action" is blank, this is a finding.

```
# authconfig --test | grep "smartcard module"
```

If any of the above checks are not configured, ask the administrator to indicate the AO-approved multifactor authentication in use and the configuration to support it. If there is no evidence of multifactor authentication, this is a finding.

Remediation:

Configure the operating system to require individuals to be authenticated with a multifactor authenticator.

Enable smartcard logons with the following commands:

```
# authconfig --enablesmartcard --smartcardaction=0 --update
# authconfig --enablerequiresmartcard -update
```

Modify the "/etc/pam_pkcs11/pkcs11_eventmgr.conf" file to uncomment the following line:

```
#/usr/X11R6/bin/xscreensaver-command -lock
```

Modify the "/etc/pam_pkcs11/pam_pkcs11.conf" file to use the cackey module if required.

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

CCI-000767 The information system implements multifactor authentication for local access to privileged accounts.

- NIST SP 800-53::IA-2 (3)
- NIST SP 800-53A::IA-2 (3).1

- NIST SP 800-53 Revision 4::IA-2 (3)

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

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

CCI-000766 Implement multifactor authentication for access to non-privileged accounts.

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

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

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)

1.62 OL07-00-020000 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must not have the rsh-server package installed.

```
GROUP ID: V-221704
RULE ID: SV-221704r958478
```

Rationale:

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

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

The rsh-server service provides an unencrypted remote access service that does not provide for the confidentiality and integrity of user passwords or the remote session and has very weak authentication.

If a privileged user were to log on using this service, the privileged user password could be compromised.

Audit:

Check to see if the rsh-server package is installed with the following command:

```
# yum list installed rsh-server
```

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

Remediation:

Configure the operating system to disable non-essential capabilities by removing the rsh-server package from the system with the following command:

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

1.63 OL07-00-020010 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must not have the ypserv package installed.

```
GROUP ID: V-221705
RULE ID: SV-221705r958478
```

Rationale:

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

Audit:

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

Check to see if the "ypserve" package is installed with the following command:

```
# yum list installed ypserv
```

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

Remediation:

Configure the operating system to disable non-essential capabilities by removing the "ypserv" package from the system with the following command:

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

1.64 OL07-00-020020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221707
RULE ID: SV-221707r958726
```

Rationale:

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

Obtain a list of authorized users for the system.

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

```
$ sudo semanage login -l | more

Login Name    SELinux User    MLS/MCS Range    Service

__default__   user_u                s0-s0:c0.c1023        *
root                  unconfined_u  s0-s0:c0.c1023        *
system_u        system_u           s0-s0:c0.c1023        *
joe                    staff_u               s0-s0:c0.c1023        *
```

All administrators must be mapped to the "staff_u", or an appropriately tailored confined SELinux user as defined by the organization.

All authorized nonadministrative users must be mapped to the "user_u" SELinux user.

If they are not mapped in this way, this is a finding.

If administrator accounts are mapped to the "sysadm_u" SELinux user and are not documented as an operational requirement with the information system security officer (ISSO), this is a finding.

If administrator accounts are mapped to the "sysadm_u" SELinux user and are documented as an operational requirement with the ISSO, this can be downgraded to a CAT III.

Remediation:

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

Use the following command to map a new user to the "staff_u" SELinux user:

```
$ sudo semanage login -a -s staff_u <username>
```

Use the following command to map an existing user to the "staff_u" SELinux user:

```
$ sudo semanage login -m -s staff_u <username>
```

Use the following command to map a new user to the "user_u" SELinux user:

```
$ sudo semanage login -a -s user_u <username>
```

Use the following command to map an existing user to the "user_u" SELinux user:

```
$ sudo semanage login -m -s user_u <username>
```

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)

1.65 OL07-00-020021 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must confine SELinux users to roles that conform to least privilege.

```
GROUP ID: V-250309
RULE ID: SV-250309r958726
```

Rationale:

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 the operating system confines SELinux users to roles that conform to least privilege.

Check the SELinux User list to SELinux Roles mapping by using the following command:

```
 $ sudo semanage user -l

                                Labeling  MLS/                MLS/
 SELinux User      Prefix       MCS Level    MCS Range           SELinux Roles

 guest_u                user          s0                     s0
guest_r
 root                         user          s0                       s0-
s0:c0.c1023    staff_r sysadm_r system_r unconfined_r
 staff_u                  user          s0                       s0-s0:c0.c1023
staff_r sysadm_r system_r unconfined_r
 sysadm_u            user          s0                     s0-s0:c0.c1023
sysadm_r
 system_u             user          s0                      s0-s0:c0.c1023
system_r unconfined_r
 unconfined_u    user          s0                     s0-s0:c0.c1023
system_r unconfined_r
 user_u                   user          s0                       s0
user_r
 xguest_u              user          s0                      s0
xguest_r
```

If the output differs from the above example, ask the system administrator (SA) to demonstrate how the SELinux User mappings are exercising least privilege. If deviations from the example are not documented with the information system security officer (ISSO) and do not demonstrate least privilege, this is a finding.

Remediation:

Configure the operating system to confine SELinux users to roles that conform to least privilege.

Use the following command to map the "staff_u" SELinux user to the "staff_r" and "sysadm_r" roles:

```
 $ sudo semanage user -m staff_u -R staff_r -R sysadm_r
```

Use the following command to map the "user_u" SELinux user to the "user_r" role:

```
 $ sudo semanage -m user_u -R user_r
```

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)

1.66 OL07-00-020022 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must not allow privileged accounts to utilize SSH.

```
GROUP ID: V-250310
RULE ID: SV-250310r958726
```

Rationale:

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

Privileged functions include, for example, establishing accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals who do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

Audit:

Verify the operating system prevents privileged accounts from utilizing SSH.

Check the SELinux ssh_sysadm_login boolean with the following command:

```
$ sudo getsebool ssh_sysadm_login
ssh_sysadm_login --> off
```

If the "ssh_sysadm_login" boolean is not "off" and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Configure the operating system to prevent privileged accounts from utilizing SSH.

Use the following command to set the "ssh_sysadm_login" boolean to "off":

```
$ sudo setsebool -P ssh_sysadm_login off
```

Note: SELinux confined users mapped to sysadm_u are not allowed to login to the system over SSH, by default. If this is a required function, it can be configured by setting the ssh_sysadm_login SELinux boolean to "on" with the following command:

```
$ sudo setsebool -P ssh_sysadm_login on
```

This must be documented with the ISSO as an operational requirement.

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)

1.67 OL07-00-020023 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must elevate the SELinux context when an administrator calls the sudo command.

```
GROUP ID: V-250311
RULE ID: SV-250311r1069170
```

Rationale:

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 the operating system 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 the operating system 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-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)

1.68 OL07-00-020028 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured to allow sending email notifications of unauthorized configuration changes to designated personnel.

```
GROUP ID: V-256977
RULE ID: SV-256977r958794
```

Rationale:

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the operating system. Changes to operating system configurations can have unintended side effects, some of which may be relevant to security.

Detecting such changes and providing an automated response can help avoid unintended, negative consequences that could ultimately affect the security state of the operating system. The operating system's IMO/ISSO and SAs must be notified via email and/or monitoring system trap when there is an unauthorized modification of a configuration item.

Audit:

Verify that the operating system is configured to allow sending email notifications.

Note: The "mailx" package provides the "mail" command that is used to send email messages.

Verify that the "mailx" package is installed on the system:

```
 $ sudo yum list installed mailx

 mailx.x86_64     12.5-19.el7     @ol7_latest
```

If "mailx" package is not installed, this is a finding.

Remediation:

Install the "mailx" package on the system:

```
 $ sudo yum install mailx
```

Additional Information:

CCI-001744 Implement organization-defined security responses automatically if baseline configurations are changed in an unauthorized manner.

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

1.69 OL07-00-020029 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must use a file integrity tool to verify correct operation of all security functions.

```
GROUP ID: V-251701
RULE ID: SV-251701r958944
```

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 the Oracle Linux operating system performing security function verification/testing and/or systems and environments that require this functionality.

Audit:

Verify that Advanced Intrusion Detection Environment (AIDE) is installed and verifies the correct operation of all security functions.

Check that the AIDE package is installed with the following command:

```
$ sudo rpm -q aide
aide-0.15.1-13.el7.x86_64
```

If AIDE is not installed, ask the System Administrator 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 yum install aide
```

Initialize it:

```
$ sudo /usr/sbin/aide --init
AIDE, version 0.15.1
### AIDE database at /var/lib/aide/aide.db.new.gz initialized.
```

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

AIDE, version 0.15.1
### All files match AIDE database. Looks okay!
```

Done.

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

1.70 OL07-00-020030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that a file integrity tool verifies the baseline operating system configuration at least weekly.

```
GROUP ID: V-221708
RULE ID: SV-221708r958794
```

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 System Security Manager (ISSM)/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.

Satisfies: SRG-OS-000363-GPOS-00150 and SRG-OS-000446-GPOS-00200

Audit:

Verify the operating system routinely checks the baseline configuration for unauthorized changes.

Note: A file integrity tool other than Advanced Intrusion Detection Environment (AIDE) may be used, but the tool must be executed at least once per week.

Check for the presence of a cron job running daily or weekly on the system that executes AIDE daily to scan for changes to the system baseline. The command used in the example will use a daily occurrence.

Check the cron directories for a script file controlling the execution of the file integrity application. For example, if AIDE is installed on the system, use the following command:

```
 # ls -al /etc/cron.* | grep aide
 -rwxr-xr-x 1 root root 602 Mar 6 20:02 aide

 # grep aide /etc/crontab /var/spool/cron/root
 /etc/crontab: 30 04 * * * root /usr/sbin/aide  --check
 /var/spool/cron/root: 30 04 * * * /usr/sbin/aide  --check
```

If the file integrity application does not exist, or a script file controlling the execution of the file integrity application does not exist, this is a finding.

Remediation:

Configure the file integrity tool to run automatically on the system at least weekly. The following example output is generic. It will set cron to run AIDE daily, but other file integrity tools may be used:

```
 # more /etc/cron.daily/aide
 #!/bin/bash

 /usr/sbin/aide --check | /bin/mail -s "$HOSTNAME - Daily AIDE integrity
check run" root@example_server_name.mil
```

Note: Per requirement OL07-00-020028, the "mailx" package must be installed on the system to enable email functionality.

Additional Information:

CCI-001744 Implement organization-defined security responses automatically if baseline configurations are changed in an unauthorized manner.

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

1.71 OL07-00-020040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that designated personnel are notified if baseline configurations are changed in an unauthorized manner.

```
GROUP ID: V-221709
RULE ID: SV-221709r958794
```

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 System Security Manager (ISSM)/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.

Audit:

Verify the operating system notifies designated personnel if baseline configurations are changed in an unauthorized manner.

Note: A file integrity tool other than Advanced Intrusion Detection Environment (AIDE) may be used, but the tool must be executed and notify specified individuals via email or an alert.

Check for the presence of a cron job running routinely on the system that executes AIDE to scan for changes to the system baseline. The commands used in the example will use a daily occurrence.

Check the cron directories for a "crontab" script file controlling the execution of the file integrity application. For example, if AIDE is installed on the system, use the following command:

```
 # ls -al /etc/cron.* | grep aide
 -rwxr-xr-x 1 root root 602 Mar 6 20:02 aide

 # grep aide /etc/crontab /var/spool/cron/root
 /etc/crontab: 30 04 * * * root /usr/sbin/aide  --check
 /var/spool/cron/root: 30 04 * * * /usr/sbin/aide  --check
```

AIDE does not have a configuration that will send a notification, so the cron job uses the mail application on the system to email the results of the file integrity run as in the following example:

```
 # more /etc/cron.daily/aide
 #!/bin/bash

 /usr/sbin/aide --check | /bin/mail -s "$HOSTNAME - Daily AIDE integrity
check run" root@example_server_name.mil
```

If the file integrity application does not notify designated personnel of changes, this is a finding.

Remediation:

Configure the operating system 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.

```
 # more /etc/cron.daily/aide

 /usr/sbin/aide --check | /bin/mail -s "$HOSTNAME - Daily AIDE integrity
check run" root@example_server_name.mil
```

Note: Per requirement OL07-00-020028, the "mailx" package must be installed on the system to enable email functionality.

Additional Information:

CCI-001744 Implement organization-defined security responses automatically if baseline configurations are changed in an unauthorized manner.

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

1.72 OL07-00-020050 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components from a repository without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.

```
GROUP ID: V-221710
RULE ID: SV-221710r1015187
```

Rationale:

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

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved CA.

Audit:

Verify the operating system prevents the installation of patches, service packs, device drivers, or operating system components from a repository without verification that they have been digitally signed using a certificate that is recognized and approved by the organization.

Check that yum verifies the signature of packages from a repository prior to install with the following command:

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

If "gpgcheck" is not set to "1", or if options are missing or commented out, ask the System Administrator how the certificates for patches and other operating system components are verified.

If there is no process to validate certificates that is approved by the organization, this is a finding.

Remediation:

Configure the operating system to verify the signature of packages from a repository prior to install by setting the following option in the "/etc/yum.conf" file:

```
gpgcheck=1
```

Additional Information:

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)

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

1.73 OL07-00-020060 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must prevent the installation of software, patches, service packs, device drivers, or operating system components of local packages without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.

```
GROUP ID: V-221711
RULE ID: SV-221711r1015188
```

Rationale:

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

Accordingly, patches, service packs, device drivers, or operating system components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This verifies the software has not been tampered with and that it has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The operating system should not have to verify the software again. This requirement does not mandate DoD certificates for this purpose; however, the certificate used to verify the software must be from an approved CA.

Audit:

Verify the operating system prevents the installation of patches, service packs, device drivers, or operating system components of local packages without verification that they have been digitally signed using a certificate that is recognized and approved by the organization.

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

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

If "localpkg_gpgcheck" is not set to "1", or if options are missing or commented out, ask the System Administrator how the signatures of local packages and other operating system components are verified.

If there is no process to validate the signatures of local packages that is approved by the organization, this is a finding.

Remediation:

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

```
localpkg_gpgcheck=1
```

Additional Information:

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)

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

1.74 OL07-00-020100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured to disable USB mass storage.

```
GROUP ID: V-221712
RULE ID: SV-221712r958498
```

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 the operating system disables the ability to load the USB Storage kernel module.

```
 # grep -r usb-storage /etc/modprobe.d/* | grep -i "/bin/false" | grep -v
"^#"
 install usb-storage /bin/false
```

If the command does not return any output, or the 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.

Verify the operating system disables the ability to use USB mass storage devices.

Check to see if USB mass storage is disabled with the following command:

```
 # grep usb-storage /etc/modprobe.d//* | grep -i "blacklist.conf" | grep -v
"^#"
 blacklist usb-storage
```

If the command does not return any output or the output is not "blacklist usb-storage", and use of USB storage devices is not documented with the ISSO as an operational requirement, this is a finding.

Remediation:

Configure the operating system to disable the ability to use the USB Storage kernel module.

Create a file under "/etc/modprobe.d" with the following command:

```
# touch /etc/modprobe.d/usb-storage.conf
```

Add the following line to the created file:

```
install usb-storage /bin/false
```

Configure the operating system to disable the ability to use USB mass storage devices.

```
# vi /etc/modprobe.d/blacklist.conf
```

Add or update the line:

```
blacklist usb-storage
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

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

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

1.75 OL07-00-020101 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that the Datagram Congestion Control Protocol (DCCP) kernel module is disabled unless required.

```
GROUP ID: V-221713
RULE ID: SV-221713r958820
```

Rationale:

Disabling DCCP protects the system against exploitation of any flaws in the protocol implementation.

Audit:

Verify the operating system disables the ability to load the DCCP kernel module.

```
# grep -r dccp /etc/modprobe.d/* | grep -i "/bin/false" | grep -v "^#"
install dccp /bin/false
```

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

Verify the operating system disables the ability to use the DCCP kernel module.

Verify the DCCP kernel module is disabled with the following command:

```
# grep -i dccp /etc/modprobe.d/* | grep -i "blacklist" | grep -v "^#"
blacklist dccp
```

If the command does not return any output or the output is not "blacklist dccp", and use of the DCCP kernel module is not documented with the ISSO as an operational requirement, this is a finding.

Remediation:

Configure the operating system to disable the ability to use the DCCP kernel module.

Create a file under "/etc/modprobe.d" with the following command:

```
# touch /etc/modprobe.d/dccp.conf
```

Add the following line to the created file:

```
install dccp /bin/false
```

Ensure that the DCCP module is blacklisted:

```
# vi /etc/modprobe.d/blacklist.conf
```

Add or update the line:

```
blacklist dccp
```

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

1.76 OL07-00-020110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must disable the file system automounter unless required.

```
GROUP ID: V-221714
RULE ID: SV-221714r958498
```

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:

Verify the operating system disables the ability to automount devices.

Check to see if automounter service is active with the following command:

```
# systemctl status autofs
autofs.service - Automounts filesystems on demand
Loaded: loaded (/usr/lib/systemd/system/autofs.service; disabled)
Active: inactive (dead)
```

If the "autofs" status is set to "active" and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Configure the operating system to disable the ability to automount devices.

Turn off the automount service with the following commands:

```
# systemctl stop autofs
# systemctl disable autofs
```

If "autofs" is required for Network File System (NFS), it must be documented with the ISSO.

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

1.77 OL07-00-020111 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must disable the graphical user interface automounter unless required.

```
GROUP ID: V-228567
RULE ID: SV-228567r958498
```

Rationale:

Automatically mounting file systems permits easy introduction of unknown devices, thereby facilitating malicious activity.

Satisfies: SRG-OS-000114-GPOS-00059, SRG-OS-000378-GPOS-00163, SRG-OS-000480-GPOS-00227

Audit:

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

Verify the operating system disables the ability to automount devices in a graphical user interface.

Note: The example below is using the database "local" for the system, so the path is "/etc/dconf/db/local.d". This path must be modified if a database other than "local" is being used.

Check to see if automounter service is disabled with the following commands:

```
# cat /etc/dconf/db/local.d/00-No-Automount


[org/gnome/desktop/media-handling]


automount=false


automount-open=false


autorun-never=true
```

If the output does not match the example above, this is a finding.

```
# cat /etc/dconf/db/local.d/locks/00-No-Automount

/org/gnome/desktop/media-handling/automount

/org/gnome/desktop/media-handling/automount-open

/org/gnome/desktop/media-handling/autorun-never
```

If the output does not match the example, this is a finding.

Remediation:

Configure the graphical user interface to disable the ability to automount devices.

Note: The example below is using the database "local" for the system, so the path is "/etc/dconf/db/local.d". This path must be modified if a database other than "local" is being used.

Create or edit the /etc/dconf/db/local.d/00-No-Automount file and add the following:

```
[org/gnome/desktop/media-handling]

automount=false

automount-open=false

autorun-never=true
```

Create or edit the /etc/dconf/db/local.d/locks/00-No-Automount file and add the following:

```
/org/gnome/desktop/media-handling/automount

/org/gnome/desktop/media-handling/automount-open

/org/gnome/desktop/media-handling/autorun-never
```

Run the following command to update the database:

```
# dconf update
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

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

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

1.78 OL07-00-020200 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

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

```
GROUP ID: V-221715
RULE ID: SV-221715r958936
```

Rationale:

Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by adversaries. Some information technology products may remove older versions of software automatically from the information system.

Audit:

Verify the operating system removes all software components after updated versions have been installed.

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

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

If "clean_requirements_on_remove" is not set to "1", "True", or "yes", or is not set in "/etc/yum.conf", this is a finding.

Remediation:

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

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

```
clean_requirements_on_remove=1
```

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)

1.79 OL07-00-020210 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must enable SELinux.

```
GROUP ID: V-221716
RULE ID: SV-221716r958944
```

Rationale:

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security function is defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

Audit:

Verify the operating system verifies correct operation of all security functions.

Check if "SELinux" is active and in "Enforcing" mode with the following command:

```
 # getenforce
 Enforcing
```

If "SELinux" is not active and not in "Enforcing" mode, this is a finding.

Remediation:

Configure the operating system to verify correct operation of all security functions.

Set the "SELinux" status and the "Enforcing" mode by modifying the "/etc/selinux/config" file to have the following line:

```
 SELINUX=enforcing
```

A reboot is required for the changes to take effect.

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-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

1.80 OL07-00-020220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must enable the SELinux targeted policy.

```
GROUP ID: V-228570
RULE ID: SV-228570r958944
```

Rationale:

Without verification of the security functions, security functions may not operate correctly and the failure may go unnoticed. Security functions are defined as the hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. Security functionality includes, but is not limited to, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters.

This requirement applies to operating systems performing security function verification/testing and/or systems and environments that require this functionality.

Audit:

Verify the operating system verifies correct operation of all security functions.

Check if "SELinux" is active and is enforcing the targeted policy with the following command:

```
# sestatus
SELinux status: enabled
SELinuxfs mount: /selinux
SELinux root directory: /etc/selinux
Loaded policy name: targeted
Current mode: enforcing
Mode from config file: enforcing
Policy MLS status: enabled
Policy deny_unknown status: allowed
Max kernel policy version: 28
```

If the "Loaded policy name" is not set to "targeted", this is a finding.

Verify that the /etc/selinux/config file is configured to the "SELINUXTYPE" to "targeted":

```
# grep -i "selinuxtype" /etc/selinux/config | grep -v '^#'
SELINUXTYPE = targeted
```

If no results are returned or "SELINUXTYPE" is not set to "targeted", this is a finding.

Remediation:

Configure the operating system to verify correct operation of all security functions.

Set the "SELinuxtype" to the "targeted" policy by modifying the "/etc/selinux/config" file to have the following line:

```
SELINUXTYPE=targeted
```

A reboot is required for the changes to take effect.

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-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

1.81 OL07-00-020230 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must be configured so that the x86 Ctrl-Alt-Delete key sequence is disabled on the command line.

```
GROUP ID: V-221717
RULE ID: SV-221717r991589
```

Rationale:

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

Audit:

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

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

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

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

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

If the ctrl-alt-del.target is active, this is a finding.

Remediation:

Configure the system to disable the Ctrl-Alt-Delete sequence for the command line with the following commands:

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

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

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.82 OL07-00-020231 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

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

```
GROUP ID: V-228565
RULE ID: SV-228565r991589
```

Rationale:

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

Audit:

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

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

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

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

logout=''
```

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

Remediation:

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

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

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

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

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.83 OL07-00-020240 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must define default permissions for all authenticated users in such a way that the user can only read and modify their own files.

```
GROUP ID: V-221718
RULE ID: SV-221718r991590
```

Rationale:

Setting the most restrictive default permissions ensures that when new accounts are created, they do not have unnecessary access.

Audit:

Verify the operating system defines default permissions for all authenticated users in such a way that the user can only read and modify their own files.

Check for the value of the "UMASK" parameter in "/etc/login.defs" file with the following command:

Note: If the value of the "UMASK" parameter is set to "000" in "/etc/login.defs" file, the Severity is raised to a CAT I.

```
# grep -i umask /etc/login.defs
UMASK 077
```

If the value for the "UMASK" parameter is not "077", or the "UMASK" parameter is missing or is commented out, this is a finding.

Remediation:

Configure the operating system to define default permissions for all authenticated users in such a way that the user can only read and modify their own files.

Add or edit the line for the "UMASK" parameter in "/etc/login.defs" file to "077":

```
UMASK 077
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.84 OL07-00-020250 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must be a vendor supported release.

```
GROUP ID: V-221719
RULE ID: SV-221719r991589
```

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.

Audit:

Verify the version of the operating system is vendor supported.

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

```
# cat /etc/oracle-release

Oracle Linux Server release 7.6
```

Current End of Premier Support for Oracle Linux 7 is Jul 2024 while Extended Support might consider extended term.

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

Remediation:

Upgrade to a supported version of the operating system.

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.85 OL07-00-020260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system security patches and updates must be installed and up to date.

```
GROUP ID: V-221720
RULE ID: SV-221720r991589
```

Rationale:

Timely patching is critical for maintaining the operational availability, confidentiality, and integrity of information technology (IT) systems. However, failure to keep operating system and application software patched is a common mistake made by IT professionals. New patches are released daily, and it is often difficult for even experienced System Administrators to keep abreast of all the new patches. When new weaknesses in an operating system exist, patches are usually made available by the vendor to resolve the problems. If the most recent security patches and updates are not installed, unauthorized users may take advantage of weaknesses in the unpatched software. The lack of prompt attention to patching could result in a system compromise.

Audit:

Verify the operating system security patches and updates are installed and up to date. Updates are required to be applied with a frequency determined by the site or Program Management Office (PMO).

Obtain the list of available package security updates from Oracle. The URL for updates is https://linux.oracle.com/errata/. It is important to note that updates provided by Oracle 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:

```
# yum history list | more
Loaded plugins: langpacks, product-id, subscription-manager
ID | Command line | Date and time | Action(s) | Altered
-------------------------------------------------------------------------------
--
70 | install aide | 2016-05-05 10:58 | Install | 1
69 | update -y | 2016-05-04 14:34 | Update | 18 EE
68 | install vlc | 2016-04-21 17:12 | Install | 21
67 | update -y | 2016-04-21 17:04 | Update | 7 EE
66 | update -y | 2016-04-15 16:47 | E, I, U | 84 EE
```

If package updates have not been performed on the system within the timeframe required by the site/program documentation, this is a finding.

Typical update frequency may be overridden by Information Assurance Vulnerability Alert (IAVA) notifications from CYBERCOM.

If the operating system is in non-compliance with the Information Assurance Vulnerability Management (IAVM) process, this is a finding.

Remediation:

Install the operating system patches or updated packages available from Oracle within 30 days or sooner as local policy dictates.

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.86 OL07-00-020270 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must not have unnecessary accounts.

```
GROUP ID: V-221721
RULE ID: SV-221721r991589
```

Rationale:

Accounts providing no operational purpose provide additional opportunities for system compromise. Unnecessary accounts include user accounts for individuals not requiring access to the system and application accounts for applications not installed on the system.

Audit:

Verify all accounts on the system are assigned to an active system, application, or user account.

Obtain the list of authorized system accounts from the Information System Security Officer (ISSO).

Check the system accounts on the system with the following command:

```
# more /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
```

Accounts such as "games" and "gopher" are not authorized accounts as they do not support authorized system functions.

If the accounts on the system do not match the provided documentation, or accounts that do not support an authorized system function are present, this is a finding.

Remediation:

Configure the system so all accounts on the system are assigned to an active system, application, or user account.

Remove accounts that do not support approved system activities or that allow for a normal user to perform administrative-level actions.

Document all authorized accounts on the system.

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.87 OL07-00-020300 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Oracle Linux operating system must be configured so that all Group Identifiers (GIDs) referenced in the /etc/passwd file are defined in the /etc/group file.

```
GROUP ID: V-221722
RULE ID: SV-221722r958482
```

Rationale:

If a user is assigned the GID of a group not existing 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 all GIDs referenced in the "/etc/passwd" file are defined in the "/etc/group" file.

Check that all referenced GIDs exist with the following command:

```
# pwck -r
```

If GIDs referenced in then "/etc/passwd" file are returned as not defined in the "/etc/group" file, this is a finding.

Remediation:

Configure the system to define all GIDs found in the "/etc/passwd" file by modifying the "/etc/group" file to add any non-existent group referenced in the "/etc/passwd" file, or change the GIDs referenced in the "/etc/passwd" file to a group that exists in "/etc/group".

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

1.88 OL07-00-020310 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must be configured so that the root account must be the only account having unrestricted access to the system.

```
GROUP ID: V-221723
RULE ID: SV-221723r991589
```

Rationale:

If an account other than root also has a User Identifier (UID) of "0", it has root authority, giving that account unrestricted access to the entire operating system. Multiple accounts with a UID of "0" afford an opportunity for potential intruders to guess a password for a privileged account.

Audit:

Check the system for duplicate UID "0" assignments with the following command:

```
# awk -F: '$3 == 0 {print $1}' /etc/passwd
```

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

1.89 OL07-00-020320 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that all files and directories have a valid owner.

```
GROUP ID: V-221724
RULE ID: SV-221724r991589
```

Rationale:

Unowned files and directories may be unintentionally inherited if a user is assigned the same User Identifier (UID) as the UID of the un-owned files.

Audit:

Verify all files and directories on the system have a valid owner.

Check the owner of all files and directories with the following command:

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

```
# find / -fstype xfs -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 the system with the "chown" command:

```
# chown <user> <file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.90 OL07-00-020330 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that all files and directories have a valid group owner.

```
GROUP ID: V-221725
RULE ID: SV-221725r991589
```

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 files and directories on the system have a valid group.

Check the owner of all files and directories with the following command:

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

```
# find / -fstype xfs -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 the system that do not have a valid group, or assign a valid group to all files and directories on the system with the "chgrp" command:

```
# chgrp <group> <file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.91 OL07-00-020610 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that all local interactive user accounts, upon creation, are assigned a home directory.

```
GROUP ID: V-221727
RULE ID: SV-221727r991589
```

Rationale:

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of owned files.

Audit:

Verify all local interactive users on the system are assigned a home directory upon creation.

Check to see if the system is configured to create home directories for local interactive users with the following command:

```
# grep -i create_home /etc/login.defs
CREATE_HOME yes
```

If the value for "CREATE_HOME" parameter is not set to "yes", the line is missing, or the line is commented out, this is a finding.

Remediation:

Configure the operating system to assign home directories to all new local interactive users by setting the "CREATE_HOME" parameter in "/etc/login.defs" to "yes" as follows.

```
CREATE_HOME yes
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.92 OL07-00-020620 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that all local interactive users have a home directory assigned and defined in the /etc/passwd file.

```
GROUP ID: V-221728
RULE ID: SV-221728r991589
```

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. In addition, 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 local interactive users on the system have a home directory assigned and the directory exists.

Check the home directory assignment for all local interactive non-privileged users on the system with the following command:

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

smithj 1001 /home/smithj
```

Note: This may miss interactive users that have been assigned a privileged UID. Evidence of interactive use may be obtained from a number of log files containing system logon information.

Check that all referenced home directories exist with the following command:

```
# pwck -r
user 'smithj': directory '/home/smithj' does not exist
```

If any home directories referenced in "/etc/passwd" are returned as not defined, or if any interactive users do not have a home directory assigned, 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 smithj, who has a home directory of "/home/smithj", a UID of "smithj", and a Group Identifier (GID) of "users" assigned in "/etc/passwd".

```
# mkdir /home/smithj
# chown smithj /home/smithj
# chgrp users /home/smithj
# chmod 0750 /home/smithj
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.93 OL07-00-020630 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that all local interactive user home directories have mode 0750 or less permissive.

```
GROUP ID: V-221729
RULE ID: SV-221729r991589
```

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.

Check the home directory assignment for all non-privileged users on the system 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.

```
# ls -ld $(awk -F: '($3>=1000)&&($7 !~ /nologin/){print $6}' /etc/passwd)

-rwxr-x--- 1 smithj users 18 Mar 5 17:06 /home/smithj
```

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 "smithj".

```
# chmod 0750 /home/smithj
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.94 OL07-00-020640 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that all local interactive user home directories are owned by their respective users.

```
GROUP ID: V-221730
RULE ID: SV-221730r991589
```

Rationale:

If a local interactive user does not own their home directory, unauthorized users could access or modify the user's files, and the users may not be able to access their own files.

Audit:

Verify the assigned home directory of all local interactive users on the system exists.

Check the home directory assignment for all local interactive users on the system with the following command:

```
# ls -ld $(awk -F: '($3>=1000)&&($7 !~ /nologin/){print $6}' /etc/passwd)

-rwxr-x--- 1 smithj users 18 Mar 5 17:06 /home/smithj
```

If any home directories referenced in "/etc/passwd" are not owned by the interactive user, this is a finding.

Remediation:

Change the owner of a local interactive user's home directories to that owner. To change the owner of a local interactive user's home directory, use the following command:

Note: The example will be for the user smithj, who has a home directory of "/home/smithj".

```
# chown smithj /home/smithj
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.95 OL07-00-020650 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that all local interactive user home directories are group-owned by the home directory owners primary group.

```
GROUP ID: V-221731
RULE ID: SV-221731r991589
```

Rationale:

If the Group Identifier (GID) of a local interactive user's home directory is not the same as the primary GID of the user, this would allow unauthorized access to the user's files, and users that share the same group may not be able to access files that they legitimately should.

Audit:

Verify the assigned home directory of all local interactive users is group-owned by that user's primary GID.

Check the home directory assignment for all local interactive users on the system with the following command:

```
# ls -ld $(awk -F: '($3>=1000)&&($7 !~ /nologin/){print $6}' /etc/passwd)

-rwxr-x--- 1 smithj users 13 Apr 1 04:20 /home/smithj
```

Check the user's primary group with the following command:

```
# grep $(grep smithj /etc/passwd | awk -F: '{print $4}') /etc/group

users:x:250:smithj,marinc,chongt
```

If the user home directory referenced in "/etc/passwd" is not group-owned by that user's primary GID, this is a finding.

Remediation:

Change the group owner of a local interactive user's home directory to the group found in "/etc/passwd". To change the group owner of a local interactive user's home directory, use the following command:

Note: The example will be for the user "smithj", who has a home directory of "/home/smithj", and has a primary group of users.

```
# chgrp users /home/smithj
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.96 OL07-00-020660 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that all files and directories contained in local interactive user home directories have a valid owner.

```
GROUP ID: V-221732
RULE ID: SV-221732r991589
```

Rationale:

Unowned files and directories may be unintentionally inherited if a user is assigned the same User Identifier "UID" as the UID of the un-owned files.

Audit:

Verify all files and directories in a local interactive user's home directory have a valid owner.

Check the owner of all files and directories in a local interactive user's home directory with the following command:

Note: The example will be for the user "smithj", who has a home directory of "/home/smithj".

```
$ sudo ls -lLR /home/smithj

-rw-r--r-- 1 smithj smithj 18 Mar 5 17:06 file1
-rw-r--r-- 1 smithj smithj 193 Mar 5 17:06 file2
-rw-r--r-- 1 smithj smithj 231 Mar 5 17:06 file3
```

If any files or directories are found without an 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 OL 7 with the "chown" command:

Note: The example will be for the user smithj, who has a home directory of "/home/smithj".

```
$ sudo chown smithj /home/smithj/<file or directory>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.97 OL07-00-020670 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that all files and directories contained in local interactive user home directories are group-owned by a group of which the home directory owner is a member.

```
GROUP ID: V-221733
RULE ID: SV-221733r991589
```

Rationale:

If a local interactive user's files are group-owned by a group of which the user is not a member, unintended users may be able to access them.

Audit:

Verify all files and directories in a local interactive user home directory are group-owned by a group of which the user is a member.

Check the group owner of all files and directories in a local interactive user's home directory with the following command:

Note: The example will be for the user "smithj", who has a home directory of "/home/smithj".

```
# ls -lLR /<home directory>/<users home directory>/
-rw-r--r-- 1 smithj smithj 18 Mar 5 17:06 file1
-rw-r--r-- 1 smithj smithj 193 Mar 5 17:06 file2
-rw-r--r-- 1 smithj sa 231 Mar 5 17:06 file3
```

If any files are found with an owner different than the group home directory user, check to see if the user is a member of that group with the following command:

```
# grep smithj /etc/group
sa:x:100:juan,shelley,bob,smithj
smithj:x:521:smithj
```

If the user is not a member of a group that group-owns file(s) in a local interactive user's home directory, this is a finding.

Remediation:

Change the group of a local interactive user's files and directories to a group that the interactive user is a member of. To change the group owner of a local interactive user's files and directories, use the following command:

Note: The example will be for the user smithj, who has a home directory of "/home/smithj" and is a member of the users group.

```
# chgrp users /home/smithj/<file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.98 OL07-00-020680 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that all files and directories contained in local interactive user home directories have a mode of 0750 or less permissive.

```
GROUP ID: V-221734
RULE ID: SV-221734r991589
```

Rationale:

If a local interactive user files have excessive permissions, unintended users may be able to access or modify them.

Audit:

Verify all files and directories contained in a local interactive user home directory, excluding local initialization files, have a mode of "0750".

Check the mode of all non-initialization files in a local interactive user home directory with the following command:

Files that begin with a "." are excluded from this requirement.

Note: The example will be for the user "smithj", who has a home directory of "/home/smithj".

```
# ls -lLR /home/smithj
-rwxr-x--- 1 smithj smithj 18 Mar 5 17:06 file1
-rwxr----- 1 smithj smithj 193 Mar 5 17:06 file2
-rw-r-x--- 1 smithj smithj 231 Mar 5 17:06 file3
```

If any files are found with a mode more permissive than "0750", this is a finding.

Remediation:

Set the mode on files and directories in the local interactive user home directory with the following command:

Note: The example will be for the user smithj, who has a home directory of "/home/smithj" and is a member of the users group.

```
# chmod 0750 /home/smithj/<file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.99 OL07-00-020690 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that all local initialization files for interactive users are owned by the home directory user or root.

```
GROUP ID: V-221735
RULE ID: SV-221735r991589
```

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 the local initialization files of all local interactive users are owned by that user.

Check the home directory assignment for all nonprivileged users on the system with the following command:

Note: The example will be for the smithj user, who has a home directory of "/home/smithj".

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

smithj 1000 /home/smithj
```

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.

```
# ls -al /home/smithj/.[^.]* | more

-rw-------. 1 smithj users 2984 Apr 27 19:02 .bash_history
-rw-r--r--. 1 smithj users   18 Aug 21  2019 .bash_logout
-rw-r--r--. 1 smithj users  193 Aug 21  2019 .bash_profile
```

If all local interactive users' initialization files are not owned by that user or root, this is a finding.

Remediation:

Set the owner of the local initialization files for interactive users to either the directory owner or root with the following command:

Note: The example will be for the smithj user, who has a home directory of "/home/smithj".

```
# chown smithj /home/smithj/.[^.]*
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.100 OL07-00-020700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that all local initialization files for local interactive users are be group-owned by the users primary group or root.

```
GROUP ID: V-221736
RULE ID: SV-221736r991589
```

Rationale:

Local initialization files for interactive users are used to configure the user's shell environment upon logon. Malicious modification of these files could compromise accounts upon logon.

Audit:

Verify the local initialization files of all local interactive users are group-owned by that user's primary Group Identifier (GID).

Check the home directory assignment for all nonprivileged users on the system with the following command:

Note: The example will be for the smithj user, who has a home directory of "/home/smithj" and a primary group of "users".

```
# awk -F: '($4>=1000)&&($7 !~ /nologin/){print $1, $4, $6}' /etc/passwd

smithj 1000 /home/smithj

# grep 1000 /etc/group

users:x:1000:smithj,jonesj,jacksons
```

Note: This may miss interactive users that have been assigned a privileged User Identifier (UID). Evidence of interactive use may be obtained from a number of log files containing system logon information.

Check the group owner of all local interactive users' initialization files with the following command:

```
# ls -al /home/smithj/.[^.]* | more

-rw-------. 1 smithj users 2984 Apr 27 19:02 .bash_history
-rw-r--r--. 1 smithj users   18 Aug 21  2019 .bash_logout
-rw-r--r--. 1 smithj users  193 Aug 21  2019 .bash_profile
```

If all local interactive users' initialization files are not group-owned by that user's primary GID, this is a finding.

Remediation:

Change the group owner of a local interactive user's files to the group found in "/etc/passwd" for the user. To change the group owner of a local interactive user's home directory, use the following command:

Note: The example will be for the user smithj, who has a home directory of "/home/smithj" and has a primary group of users.

```
# chgrp users /home/smithj/.[^.]*
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.101 OL07-00-020710 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that all local initialization files have mode 0740 or less permissive.

```
GROUP ID: V-221737
RULE ID: SV-221737r991589
```

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.

Check the mode on all local initialization files with the following command:

Note: The example will be for the "smithj" user, who has a home directory of "/home/smithj".

```
 # ls -al /home/smithj/.[^.]* | more

 -rw-------. 1 smithj users 2984 Apr 27 19:02 .bash_history
 -rw-r--r--. 1 smithj users   18 Aug 21  2019 .bash_logout
 -rw-r--r--. 1 smithj users  193 Aug 21  2019 .bash_profile
```

If any local initialization files have a mode more permissive than "0740", this is a finding.

Remediation:

Set the mode of the local initialization files to "0740" with the following command:

Note: The example will be for the "smithj" user, who has a home directory of "/home/smithj".

```
 # chmod 0740 /home/smithj/.[^.]*
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.102 OL07-00-020720 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that all local interactive user initialization files executable search paths contain only paths that resolve to the users home directory.

```
GROUP ID: V-221738
RULE ID: SV-221738r991589
```

Rationale:

The executable search path (typically the PATH environment variable) contains a list of directories for the shell to search to find executables. If this path includes the current working directory (other than the user's home directory), executables in these directories may be executed instead of system commands. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is interpreted as the current working directory. If deviations from the default system search path for the local interactive user are required, they must be documented with the Information System Security Officer (ISSO).

Audit:

Verify that all local interactive user initialization files' executable search path statements do not contain statements that will reference a working directory other than the users' home directory.

Check the executable search path statement for all local interactive user initialization files in the users' home directory with the following commands:

Note: The example will be for the smithj user, which has a home directory of "/home/smithj".

```
# grep -i path= /home/smithj/.*
/home/smithj/.bash_profile:PATH=$PATH:$HOME/.local/bin:$HOME/bin
```

If any local interactive user initialization files have executable search path statements that include directories outside of their home directory, 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 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.103 OL07-00-020730 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that local initialization files do not execute world-writable programs.

```
GROUP ID: V-221739
RULE ID: SV-221739r991589
```

Rationale:

If user start-up files execute world-writable programs, especially in unprotected directories, they could be maliciously modified to destroy user files or otherwise compromise the system at the user level. If the system is compromised at the user level, it is easier to elevate privileges to eventually compromise the system at the root and network level.

Audit:

Verify that local initialization files do not execute world-writable programs.

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

```
# find / -xdev -perm -002 -type f -exec ls -ld {} \; | more
```

For all files listed, check for their presence in the local initialization files with the following commands:

Note: The example will be for a system that is configured to create users' home directories in the "/home" directory.

```
# grep <file> /home/*/.*
```

If any local initialization files are found to reference world-writable files, this is a finding.

Remediation:

Set the mode on files being executed by the local initialization files with the following command:

```
# chmod 0755 <file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.104 OL07-00-020900 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221740
RULE ID: SV-221740r991589
```

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:

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

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

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

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

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

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

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.105 OL07-00-021000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221741
RULE ID: SV-221741r991589
```

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 unprivileged users to attain unauthorized administrative access.

Audit:

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

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

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

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

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

```
# more /etc/fstab

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

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

Remediation:

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

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.106 OL07-00-021010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system 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-221742
RULE ID: SV-221742r991589
```

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 unprivileged users to attain unauthorized administrative access.

Audit:

Verify file systems used for removable media are mounted with the "nosuid" option.

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

```
# more /etc/fstab

UUID=2bc871e4-e2a3-4f29-9ece-3be60c835222 /mnt/usbflash vfat
noauto,owner,ro,nosuid 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 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.107 OL07-00-021020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must prevent files with the setuid and setgid bit set from being executed on file systems that are being imported via Network File System (NFS).

```
GROUP ID: V-221743
RULE ID: SV-221743r991589
```

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 unprivileged users to attain unauthorized administrative access.

Audit:

Verify file systems being NFS imported are configured with the "nosuid" option.

Find the file system(s) that contain the directories being exported with the following command:

```
# more /etc/fstab | grep nfs

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

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

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

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

If no results are returned, this is a finding.

Remediation:

Configure the "/etc/fstab" 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 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.108 OL07-00-021021 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221744
RULE ID: SV-221744r991589
```

Rationale:

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

Audit:

Verify file systems that are being NFS imported are configured with the "noexec" option.

Find the file system(s) that contain the directories being imported with the following command:

```
# more /etc/fstab | grep nfs

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

If a file system found in "/etc/fstab" refers to NFS and it does not have the "noexec" option set, and use of NFS imported binaries is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

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

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

If no results are returned and use of NFS imported binaries is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Configure the "/etc/fstab" 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 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.109 OL07-00-021024 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Oracle Linux operating system must mount /dev/shm with secure options.

```
GROUP ID: V-221747
RULE ID: SV-221747r958804
```

Rationale:

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

Audit:

Verify that the "nodev","nosuid", and "noexec" options are configured for /dev/shm:

```
# cat /etc/fstab | grep /dev/shm

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

If results are returned and the "nodev","nosuid", or "noexec" options are missing, this is a finding.

Verify "/dev/shm" is mounted with the "nodev","nosuid", and "noexec" options:

```
# mount | grep /dev/shm

tmpfs on /dev/shm type tmpfs (rw,nodev,nosuid,noexec,seclabel)
```

If /dev/shm is mounted without secure options "nodev", "nosuid", and "noexec", this is a finding.

Remediation:

Configure the system so that /dev/shm is mounted with the "nodev", "nosuid", and "noexec" options by adding /modifying the /etc/fstab with the following line:

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

1.110 OL07-00-021030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221748
RULE ID: SV-221748r991589
```

Rationale:

If a world-writable directory is not group-owned by root, sys, bin, or an application Group Identifier (GID), unauthorized users may be able to modify files created by others.

The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage, (e.g., /tmp), and for directories requiring global read/write access.

Audit:

The following command will discover and print world-writable directories that are not group-owned by a system account, given the assumption that only system accounts have a gid lower than 1000. Run it once for each local partition [PART]:

```
# find [PART] -xdev -type d -perm -0002 -gid +999 -print
```

If there is output, this is a finding.

Remediation:

All directories in local partitions which are world-writable should be group-owned by root or another system account. If any world-writable directories are not group-owned by a system account, this should be investigated. Following this, the directories should be deleted or assigned to an appropriate group.

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.111 OL07-00-021031 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-228566
RULE ID: SV-228566r991589
```

Rationale:

If a world-writable directory is not owned by root, sys, bin, or an application User Identifier (UID), unauthorized users may be able to modify files created by others.

The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage, (e.g., /tmp), and for directories requiring global read/write access.

Audit:

The following command will discover and print world-writable directories that are not owned by a system account, assuming that only system accounts have a UID lower than 1000. Run it once for each local partition [PART]:

```
# find [PART] -xdev -type d -perm -0002 -uid +999 -print
```

If there is output, this is a finding.

Remediation:

All directories in local partitions which are world-writable should be owned by root or another system account. If any world-writable directories are not owned by a system account, this should be investigated. Following this, the files should be deleted or assigned to an appropriate group.

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.112 OL07-00-021040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must set the umask value to 077 for all local interactive user accounts.

```
GROUP ID: V-221749
RULE ID: SV-221749r991589
```

Rationale:

The umask controls the default access mode assigned to newly created files. A umask of 077 limits new files to mode 700 or less permissive. Although umask can be represented as a four-digit number, the first digit representing special access modes is typically ignored or required to be "0". This requirement applies to the globally configured system defaults and the local interactive user defaults for each account on the system.

Audit:

Verify that the default umask for all local interactive users is "077".

Identify the locations of all local interactive user home directories by looking at the "/etc/passwd" file.

Check all local interactive user initialization files for interactive users with the following command:

Note: The example is for a system that is configured to create users home directories in the "/home" directory.

```
$ sudo grep -ir ^umask /home | grep -v '.bash_history'
```

If any local interactive user initialization files are found to have a umask statement that has a value less restrictive than "077", this is a finding.

Remediation:

Remove the umask statement from all local interactive user's initialization files.

If the account is for an application, the requirement for a umask less restrictive than "077" can be documented with the Information System Security Officer, but the user agreement for access to the account must specify that the local interactive user must log on to their account first and then switch the user to the application account with the correct option to gain the account's environment variables.

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.113 OL07-00-021100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must have cron logging implemented.

```
GROUP ID: V-221750
RULE ID: SV-221750r991589
```

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.

Check the configuration of "/etc/rsyslog.conf" or "/etc/rsyslog.d/*.conf" files for the cron facility 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 cron /etc/rsyslog.conf /etc/rsyslog.d/*.conf
cron.* /var/log/cron
```

If the command does not return a response, check for cron logging all facilities by inspecting the "/etc/rsyslog.conf" or "/etc/rsyslog.d/*.conf" files.

Look for the following entry:

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

1.114 OL07-00-021110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that the cron.allow file, if it exists, is owned by root.

```
GROUP ID: V-221751
RULE ID: SV-221751r991589
```

Rationale:

If the owner of the "cron.allow" file is not set to root, the possibility exists for an unauthorized user to view or to edit sensitive information.

Audit:

Verify that the "cron.allow" file is owned by root.

Check the owner of the "cron.allow" file with the following command:

```
# ls -al /etc/cron.allow
-rw------- 1 root root 6 Mar 5 2011 /etc/cron.allow
```

If the "cron.allow" file exists and has an owner other than root, this is a finding.

Remediation:

Set the owner on the "/etc/cron.allow" file to root with the following command:

```
# chown root /etc/cron.allow
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.115 OL07-00-021120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that the cron.allow file, if it exists, is group-owned by root.

```
GROUP ID: V-221752
RULE ID: SV-221752r991589
```

Rationale:

If the group owner of the "cron.allow" file is not set to root, sensitive information could be viewed or edited by unauthorized users.

Audit:

Verify that the "cron.allow" file is group-owned by root.

Check the group owner of the "cron.allow" file with the following command:

```
# ls -al /etc/cron.allow
-rw------- 1 root root 6 Mar 5 2011 /etc/cron.allow
```

If the "cron.allow" file exists and has a group owner other than root, this is a finding.

Remediation:

Set the group owner on the "/etc/cron.allow" file to root with the following command:

```
# chgrp root /etc/cron.allow
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.116 OL07-00-021300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must disable Kernel core dumps unless needed.

```
GROUP ID: V-221753
RULE ID: SV-221753r991589
```

Rationale:

Kernel core dumps may contain the full contents of system memory at the time of the crash. Kernel core dumps may consume a considerable amount of disk space, and may result in denial of service by exhausting the available space on the target file system partition.

Audit:

Verify that kernel core dumps are disabled unless needed.

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

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

If the "kdump" service is active, ask the System Administrator if the use of the service is required and documented with the Information System Security Officer (ISSO).

If the service is active and is not documented, this is a finding.

Remediation:

If kernel core dumps are not required, disable the "kdump" service with the following command:

```
# systemctl disable kdump.service
```

If kernel core dumps are required, document the need with the ISSO.

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.117 OL07-00-021310 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Oracle Linux operating system must be configured so that a separate file system is used for user home directories (such as /home or an equivalent).

```
GROUP ID: V-221754
RULE ID: SV-221754r991589
```

Rationale:

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

Audit:

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

Check the home directory assignment for all non-privileged users (those with a UID of 1000 or greater) on the system with the following command:

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

adamsj 1000 /home/adamsj /bin/bash
jacksonm 1001 /home/jacksonm /bin/bash
smithj 1002 /home/smithj /bin/bash
```

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

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

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

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

If a separate entry for the file system/partition that contains the non-privileged interactive users' home directories does not exist, 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 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.118 OL07-00-021320 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Oracle Linux operating system must use a separate file system for /var.

```
GROUP ID: V-221755
RULE ID: SV-221755r991589
```

Rationale:

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

Audit:

Verify that a separate file system/partition has been created for "/var".

Check that a file system/partition has been created for "/var" with the following command:

```
# grep /var /etc/fstab
UUID=c274f65f /var ext4 noatime,nobarrier 1 2
```

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

1.119 OL07-00-021330 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Oracle Linux operating system must use a separate file system for the system audit data path large enough to hold at least one week of audit data.

```
GROUP ID: V-221756
RULE ID: SV-221756r958752
```

Rationale:

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

Audit:

Determine if the operating system is configured to have the "/var/log/audit" path is on a separate file system.

```
# grep /var/log/audit /etc/fstab
```

If no result is returned, or the operating system is not configured to have "/var/log/audit" on a separate file system, this is a finding.

Verify that "/var/log/audit" is mounted on a separate file system:

```
# mount | grep "/var/log/audit"
```

If no result is returned, or "/var/log/audit" is not on a separate file system, this is a finding.

Verify the size of the audit file system:

```
# df -h /var/log/audit
```

If the size is insufficient for a week of audit data, this is a finding.

Remediation:

Migrate the system audit data path onto an appropriately sized separate file system to store at least one week of audit records.

Additional Information:

CCI-001849 Allocate audit log storage capacity to accommodate organization-defined audit log retention requirements.

- NIST SP 800-53 Revision 4::AU-4
- NIST SP 800-53 Revision 5::AU-4

1.120 OL07-00-021340 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Oracle Linux operating system must use a separate file system for /tmp (or equivalent).

```
GROUP ID: V-221757
RULE ID: SV-221757r991589
```

Rationale:

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

Audit:

Verify that a separate file system/partition has been created for "/tmp".

Check that a file system/partition has been created for "/tmp" with the following command:

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

If the "tmp.mount" service is not enabled, check to see if "/tmp" is defined in the fstab with a device and mount point:

```
# grep -i /tmp /etc/fstab
UUID=a411dc99-f2a1-4c87-9e05-184977be8539 /tmp ext4
rw,relatime,discard,data=ordered,nosuid,noexec, 0 0
```

If "tmp.mount" service is not enabled or the "/tmp" directory is not defined in the fstab with a device and mount point, this is a finding.

Remediation:

Start the "tmp.mount" service with the following command:

```
# systemctl enable tmp.mount
```

OR

Edit the "/etc/fstab" file and ensure the "/tmp" directory is defined in the fstab with a device and mount point.

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.121 OL07-00-021350 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must implement NIST FIPS-validated cryptography for the following: to provision digital signatures, to generate cryptographic hashes, and to protect data requiring data-at-rest protections in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

```
GROUP ID: V-221758
RULE ID: SV-221758r958408
```

Rationale:

Use of weak or untested encryption algorithms undermines the purposes of using encryption to protect data. The operating system must implement cryptographic modules that adhere to the higher standards approved by the federal government to ensure they have been tested and validated.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000185-GPOS-00079, SRG-OS-000396-GPOS-00176, SRG-OS-000405-GPOS-00184, SRG-OS-000478-GPOS-00223

Audit:

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

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

```
# yum list installed dracut-fips

dracut-fips-033-360.el7_2.x86_64.rpm
```

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

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

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

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

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

If a "dracut-fips" package is not installed, the kernel command line does not have a fips entry, or the system has a value of "0" for "fips_enabled" in "/proc/sys/crypto", this is a finding.

Verify the file /etc/system-fips exists.

```
# ls -l /etc/system-fips
```

If this file does not exist, this is a finding.

Remediation:

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

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

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

The fips=1 kernel option needs to be added to the kernel command line during system installation so that key generation is done with FIPS-approved algorithms and continuous monitoring tests in place. Users should also ensure that the system has plenty of entropy during the installation process by moving the mouse around, or if no mouse is available, ensuring that many keystrokes are typed. The recommended amount of keystrokes is 256 and more. Less than 256 keystrokes may generate a non-unique key.

Install the dracut-fips package with the following command:

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

Recreate the "initramfs" file with the following command:

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

```
# dracut -f
```

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

```
fips=1
```

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

On BIOS-based machines, use the following command:

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

On UEFI-based machines, use the following command:

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

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

```
# df /boot

Filesystem 1K-blocks Used Available Use% Mounted on

/dev/sda1 495844 53780 416464 12% /boot
```

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

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

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

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

If the file /etc/system-fips does not exists, recreate it:

```
# touch /etc/ system-fips
```

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 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

CCI-001199 Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

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-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)

1.122 OL07-00-021600 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Oracle Linux operating system must be configured so that the file integrity tool is configured to verify Access Control Lists (ACLs).

```
GROUP ID: V-221759
RULE ID: SV-221759r991589
```

Rationale:

ACLs can provide permissions beyond those permitted through the file mode and must be verified by file integrity tools.

Audit:

Verify the file integrity tool is configured to verify ACLs.

Note: AIDE is highly configurable at install time. These commands assume the "aide.conf" file is under the "/etc" directory.

Use the following command to determine if the file is in another location:

```
 # find / -name aide.conf
```

Check the "aide.conf" file to determine if the "acl" rule has been added to the rule list being applied to the files and directories selection lists.

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

```
 All= p+i+n+u+g+s+m+S+sha512+acl+xattrs+selinux
 /bin All # apply the custom rule to the files in bin
 /sbin All # apply the same custom rule to the files in sbin
```

If the "acl" rule is not being used on all uncommented selection lines in the "/etc/aide.conf" file, or ACLs are not being checked by another file integrity tool, 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 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.123 OL07-00-021610 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

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

```
GROUP ID: V-221760
RULE ID: SV-221760r991589
```

Rationale:

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

Audit:

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

Note: AIDE is highly configurable at install time. These commands assume the "aide.conf" file is under the "/etc" directory.

Use the following command to determine if the file is in another location:

find / -name aide.conf

Check the "aide.conf" file to determine if the "xattrs" rule has been added to the rule list being applied to the files and directories selection lists.

An example rule that includes the "xattrs" rule follows:

```
 All= p+i+n+u+g+s+m+S+sha512+acl+xattrs+selinux
 /bin All # apply the custom rule to the files in bin
 /sbin All # apply the same custom rule to the files in sbin
```

If the "xattrs" rule is not being used on all uncommented selection lines in the "/etc/aide.conf" file, or extended attributes are not being checked by another file integrity tool, 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 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.124 OL07-00-021620 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221761
RULE ID: SV-221761r991589
```

Rationale:

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

Audit:

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

Note: AIDE is highly configurable at install time. These commands assume the "aide.conf" file is under the "/etc" directory.

Use the following command to determine if the file is in another location:

```
 # find / -name aide.conf
```

Check the "aide.conf" file to determine if the "sha512" rule has been added to the rule list being applied to the files and directories selection lists. Exclude any log files, or files expected to change frequently, to reduce unnecessary notifications.

An example rule that includes the "sha512" rule follows:

```
 All=p+i+n+u+g+s+m+S+sha512+acl+xattrs+selinux
 /bin All # apply the custom rule to the files in bin
 /sbin All # apply the same custom rule to the files in sbin
```

If the "sha512" rule is not being used on all uncommented selection lines in the "/etc/aide.conf" file, or another file integrity tool is not using FIPS 140-2-approved cryptographic hashes for validating file contents and directories, this is a finding.

Remediation:

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

If AIDE is installed, ensure the "sha512" rule is present on all uncommented file and directory selection lists. 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 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.125 OL07-00-021700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221762
RULE ID: SV-221762r958796
```

Rationale:

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

Audit:

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

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

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

```
 # find / -name grub.cfg
 /boot/efi/EFI/redhat/grub.cfg
```

If a "grub.cfg" is found in any subdirectories other than "/boot/grub2/" and "/boot/efi/EFI/redhat/", ask the system administrator (SA) if there is documentation signed by the information system security officer (ISSO) to approve the use of removable media as a boot loader.

List the number of menu entries defined in the grub configuration file with the following command (the number will vary between systems):

```
 # grep -cw menuentry /boot/efi/EFI/redhat/grub.cfg
 4
```

Check that the grub configuration file has the "set root" command for each menu entry with the following command ("set root" defines the disk and partition or directory where the kernel and GRUB 2 modules are stored):

```
# grep 'set root' /boot/efi/EFI/redhat/grub.cfg
set root='hd0,gpt2'
set root='hd0,gpt2'
set root='hd0,gpt2'
set root='hd0,gpt2'
```

If the system is using an alternate boot loader on removable media, and documentation does not exist approving the alternate configuration, this is a finding.

Remediation:

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

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)

1.126 OL07-00-021710 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must not have the telnet-server package installed.

```
GROUP ID: V-221763
RULE ID: SV-221763r958478
```

Rationale:

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

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

Examples of non-essential capabilities include, but are not limited to, games, software packages, tools, and demonstration software not related to requirements or providing a wide array of functionality not required for every mission, but which cannot be disabled.

Audit:

Verify the operating system is configured to disable non-essential capabilities. The most secure way of ensuring a non-essential capability is disabled is not to install the capability.

The telnet service provides an unencrypted remote access service 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.

Check to see if the telnet-server package is installed with the following command:

```
# yum list installed telnet-server
```

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

Remediation:

Configure the operating system to disable non-essential capabilities by removing the telnet-server package from the system with the following command:

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

1.127 OL07-00-030000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that auditing is configured to produce records containing information to establish what type of events occurred, where the events occurred, the source of the events, and the outcome of the events. These audit records must also identify individual identities of group account users.

```
GROUP ID: V-221764
RULE ID: SV-221764r1015189
```

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.

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 the operating system audit logs provides a means of investigating an attack; recognizing resource utilization or capacity thresholds, or identifying an improperly configured operating system.

Satisfies: SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000042-GPOS-00021, SRG-OS-000254-GPOS-00095, SRG-OS-000365-GPOS-00152, SRG-OS-000255-GPOS-00096

Audit:

Verify the operating system produces audit records containing information to establish when (date and time) the events occurred.

Check to see if auditing is active by issuing the following command:

```
# systemctl is-active auditd.service
active
```

If the "auditd" status is not active, this is a finding.

Remediation:

Configure the operating system to produce audit records containing information to establish when (date and time) the events occurred.

Enable the auditd service with the following command:

```
# systemctl start auditd.service
```

Additional Information:

CCI-000131 Ensure that audit records containing information that establishes when the event occurred.

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

CCI-000132 Ensure that audit records containing information that establishes where the event occurred.

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

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

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

- NIST SP 800-53::AU-14 (1)
- NIST SP 800-53A::AU-14 (1).1
- NIST SP 800-53 Revision 4::AU-14 (1)
- NIST SP 800-53 Revision 5::AU-14 (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 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3

- NIST SP 800-53 Revision 5::AU-3 f

CCI-001814 The Information system supports auditing of the enforcement actions.

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

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

1.128 OL07-00-030010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must shut down upon audit processing failure, unless availability is an overriding concern. If availability is a concern, the system must alert the designated staff (System Administrator [SA] and Information System Security Officer [ISSO] at a minimum) in the event of an audit processing failure.

```
GROUP ID: V-221765
RULE ID: SV-221765r958424
```

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-000047-GPOS-00023

Audit:

Confirm the audit configuration regarding how auditing processing failures are handled.

Check to see what level "auditctl" is set to with following command:

```
# auditctl -s | grep -i "fail"

failure 2
```

Note: If the value of "failure" is set to "2", the system is configured to panic (shut down) in the event of an auditing failure. If the value of "failure" is set to "1", the system will not shut down and instead will record the audit failure in the kernel log. If the system is configured per requirement OL07-00-031000, the kernel log will be sent to a log aggregation server and generate an alert.

If the "failure" setting is set to any value other than "1" or "2", this is a finding.

If the "failure" setting is not set, this must be upgraded to a CAT I finding.

If the "failure" setting is set to "1" but the availability concern is not documented or there is no monitoring of the kernel log, this must be downgraded to a CAT III finding.

Remediation:

Configure the operating system to shut down in the event of an audit processing failure.

Add or correct the option to shut down the operating system with the following command:

```
# auditctl -f 2
```

Edit the "/etc/audit/rules.d/audit.rules" file and add the following line:

```
-f 2
```

If availability has been determined to be more important, and this decision is documented with the ISSO, configure the operating system to notify system administration staff and ISSO staff in the event of an audit processing failure with the following command:

```
# auditctl -f 1
```

Edit the "/etc/audit/rules.d/audit.rules" file and add the following line:

```
-f 1
```

Kernel log monitoring must also be configured to properly alert designated staff.

The audit daemon must be restarted for the 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 800-53A::AU-5.1 (ii)
- NIST SP 800-53 Revision 4::AU-5 a
- NIST SP 800-53 Revision 5::AU-5 a

1.129 OL07-00-030201 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured to off-load audit logs onto a different system or storage media from the system being audited.

```
GROUP ID: V-221767
RULE ID: SV-221767r958754
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

One method of off-loading audit logs in Oracle Linux is with the use of the audisp-remote dameon. Without the configuration of the "au-remote" plugin, the audisp-remote daemon will not off load the logs from the system being audited.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Audit:

Verify the "au-remote" plugin is configured to always off-load audit logs using the audisp-remote daemon:

```
# cat /etc/audisp/plugins.d/au-remote.conf | grep -v "^#"



active = yes

direction = out

path = /sbin/audisp-remote

type = always

format = string
```

If "active" is not set to "yes", "direction" is not set to "out", "path" is not set to "/sbin/audisp-remote", "type is not set to "always", or any of the lines are commented out, ask the System Administrator to indicate how the audit logs are off-loaded to a different system or storage media.

If there is no evidence that the system is configured to off-load audit logs to a different system or storage media, this is a finding.

Remediation:

Edit the /etc/audisp/plugins.d/au-remote.conf file and add or update the following values:

```
active = yes
direction = out
path = /sbin/audisp-remote
type = always
```

The audit daemon must be restarted for changes to take effect:

```
# service auditd restart
```

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)

1.130 OL07-00-030210 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must take appropriate action when the remote logging buffer is full.

```
GROUP ID: V-221768
RULE ID: SV-221768r958754
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

One method of off-loading audit logs in Oracle Linux is with the use of the audisp-remote dameon. When the remote buffer is full, audit logs will not be collected and sent to the central log server.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Audit:

Verify the audisp daemon is configured to take an appropriate action when the internal queue is full:

```
# grep "overflow_action" /etc/audisp/audispd.conf

overflow_action = syslog
```

If the "overflow_action" option is not "syslog", "single", or "halt", or the line is commented out, ask the System Administrator to indicate how the audit logs are off-loaded to a different system or storage media, and to indicate what action the system takes when the internal queue is full.

If there is no evidence that the system is configured to off-load audit logs to a different system or storage media, or if the configuration does not take appropriate action when the internal queue is full, this is a finding.

Remediation:

Edit the /etc/audisp/audispd.conf file and add or update the "overflow_action" option:

```
overflow_action = syslog
```

The audit daemon must be restarted for changes to take effect:

```
# service auditd restart
```

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)

1.131 OL07-00-030211 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must label all off-loaded audit logs before sending them to the central log server.

```
GROUP ID: V-221769
RULE ID: SV-221769r958754
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

One method of off-loading audit logs in Oracle Linux is with the use of the audisp-remote dameon. 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-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Audit:

Verify the audisp daemon is configured to label all off-loaded audit logs:

```
# grep "name_format" /etc/audisp/audispd.conf



name_format = hostname
```

If the "name_format" option is not "hostname", "fqd", or "numeric", or the line is commented out, ask the System Administrator to indicate how the audit logs are off-loaded to a different system or storage media, and to indicate if the logs are labeled appropriately.

If there is no evidence that the system is configured to off-load audit logs to a different system or storage media, or if the configuration does not appropriately label logs before they are off-loaded, this is a finding.

Remediation:

Edit the /etc/audisp/audispd.conf file and add or update the "name_format" option:

```
name_format = hostname
```

The audit daemon must be restarted for changes to take effect:

```
# service auditd restart
```

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)

1.132 OL07-00-030300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must off-load audit records onto a different system or media from the system being audited.

```
GROUP ID: V-221770
RULE ID: SV-221770r958754
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Audit:

Verify the operating system off-loads audit records onto a different system or media from the system being audited.

To determine the remote server that the records are being sent to, use the following command:

```
# grep -i remote_server /etc/audisp/audisp-remote.conf
remote_server = 10.0.21.1
```

If a remote server is not configured, or the line is commented out, ask the System Administrator to indicate how the audit logs are off-loaded to a different system or media.

If there is no evidence that the audit logs are being off-loaded to another system or media, this is a finding.

Remediation:

Configure the operating system to off-load audit records onto a different system or media from the system being audited.

Set the remote server option in "/etc/audisp/audisp-remote.conf" with the IP address of the log aggregation server.

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)

1.133 OL07-00-030310 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must encrypt the transfer of audit records off-loaded onto a different system or media from the system being audited.

```
GROUP ID: V-221771
RULE ID: SV-221771r958754
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Satisfies: SRG-OS-000342-GPOS-00133, SRG-OS-000479-GPOS-00224

Audit:

Verify the operating system encrypts audit records off-loaded onto a different system or media from the system being audited.

To determine if the transfer is encrypted, use the following command:

```
# grep -i enable_krb5 /etc/audisp/audisp-remote.conf
enable_krb5 = yes
```

If the value of the "enable_krb5" option is not set to "yes" or the line is commented out, ask the System Administrator to indicate how the audit logs are off-loaded to a different system or media.

If there is no evidence that the transfer of the audit logs being off-loaded to another system or media is encrypted, this is a finding.

Remediation:

Configure the operating system to encrypt the transfer of off-loaded audit records onto a different system or media from the system being audited.

Uncomment the "enable_krb5" option in "/etc/audisp/audisp-remote.conf" and set it with the following line:

```
enable_krb5 = yes
```

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)

1.134 OL07-00-030320 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that the audit system takes appropriate action when the audit storage volume is full.

```
GROUP ID: V-221772
RULE ID: SV-221772r958754
```

Rationale:

Taking appropriate action in case of a filled audit storage volume will minimize the possibility of losing audit records. One method of off-loading audit logs in Oracle Linux is with the use of the audisp-remote dameon.

Audit:

Verify the action the operating system takes if the disk the audit records are written to becomes full.

To determine the action that takes place if the disk is full on the remote server, use the following command:

```
# grep -i disk_full_action /etc/audisp/audisp-remote.conf
disk_full_action = single
```

If the value of the "disk_full_action" option is not "syslog", "single", or "halt", or the line is commented out, ask the System Administrator to indicate how the audit logs are off-loaded to a different system or storage media, and to indicate the action taken when the disk is full on the remote server.

If there is no evidence that the system is configured to off-load audit logs to a different system or storage media, or if the configuration does not take appropriate action when the disk is full on the remote server, this is a finding.

Remediation:

Configure the action the operating system takes if the disk the audit records are written to becomes full.

Uncomment or edit the "disk_full_action" option in "/etc/audisp/audisp-remote.conf" and set it to "syslog", "single", or "halt", such as the following line:

```
disk_full_action = single
```

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)

1.135 OL07-00-030321 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that the audit system takes appropriate action when there is an error sending audit records to a remote system.

```
GROUP ID: V-221773
RULE ID: SV-221773r958754
```

Rationale:

Taking appropriate action when there is an error sending audit records to a remote system will minimize the possibility of losing audit records. One method of off-loading audit logs in Oracle Linux is with the use of the audisp-remote dameon.

Audit:

Verify the action the operating system takes if there is an error sending audit records to a remote system.

Check the action that takes place if there is an error sending audit records to a remote system with the following command:

```
# grep -i network_failure_action /etc/audisp/audisp-remote.conf
network_failure_action = syslog
```

If the value of the "network_failure_action" option is not "syslog", "single", or "halt", or the line is commented out, ask the System Administrator to indicate how the audit logs are off-loaded to a different system or storage media, and to indicate the action taken if there is an error sending audit records to the remote system.

If there is no evidence that the system is configured to off-load audit logs to a different system or storage media, or if the configuration does not take appropriate action if there is an error sending audit records to the remote system, this is a finding.

Remediation:

Configure the action the operating system takes if there is an error sending audit records to a remote system.

Uncomment the "network_failure_action" option in "/etc/audisp/audisp-remote.conf" and set it to "syslog", "single", or "halt".

```
network_failure_action = syslog
```

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)

1.136 OL07-00-030330 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must initiate an action to notify the System Administrator (SA) and Information System Security Officer (ISSO), at a minimum, when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity.

```
GROUP ID: V-221774
RULE ID: SV-221774r971542
```

Rationale:

If security personnel are not notified immediately when storage volume reaches 75 percent utilization, they are unable to plan for audit record storage capacity expansion.

Audit:

Verify the operating system initiates an action to notify the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity.

Check the system configuration to determine the partition the audit records are being written to with the following command:

```
$ sudo grep -iw log_file /etc/audit/auditd.conf

log_file = /var/log/audit/audit.log
```

Determine what the threshold is for the system to take action when 75 percent of the repository maximum audit record storage capacity is reached:

```
$ sudo grep -iw 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 total partition size, this is a finding.

Remediation:

Configure the operating system to initiate an action to notify the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity.

Set the value of the "space_left" keyword in "/etc/audit/auditd.conf" to 25 percent of the partition size.

```
space_left = 25%
```

Reload the auditd daemon to apply changes made to the "/etc/audit/auditd.conf" file.

```
$ sudo service auditd restart
```

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)

1.137 OL07-00-030340 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must immediately notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) via email when the threshold for the repository maximum audit record storage capacity is reached.

```
GROUP ID: V-221775
RULE ID: SV-221775r971542
```

Rationale:

If security personnel are not notified immediately when the threshold for the repository maximum audit record storage capacity is reached, they are unable to expand the audit record storage capacity before records are lost.

Audit:

Verify the operating system immediately notifies the SA and ISSO (at a minimum) via email when the allocated audit record storage volume reaches 75 percent of the repository maximum audit record storage capacity.

Check what action the operating system takes when the threshold for the repository maximum audit record storage capacity is reached with the following command:

```
# grep -i space_left_action /etc/audit/auditd.conf
space_left_action = email
```

If the value of the "space_left_action" keyword is not set to "email", this is a finding.

Remediation:

Configure the operating system to immediately notify the SA and ISSO (at a minimum) when the threshold for the repository maximum audit record storage capacity is reached.

Uncomment or edit the "space_left_action" keyword in "/etc/audit/auditd.conf" and set it to "email".

```
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)

1.138 OL07-00-030350 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must immediately notify the System Administrator (SA) and Information System Security Officer (ISSO) (at a minimum) when the threshold for the repository maximum audit record storage capacity is reached.

```
GROUP ID: V-221776
RULE ID: SV-221776r971542
```

Rationale:

If security personnel are not notified immediately when the threshold for the repository maximum audit record storage capacity is reached, they are unable to expand the audit record storage capacity before records are lost.

Audit:

Verify the operating system immediately notifies the SA and ISSO (at a minimum) via email when the threshold for the repository maximum audit record storage capacity is reached.

Check what account the operating system emails when the threshold for the repository maximum audit record storage capacity is reached with the following command:

```
# grep -i 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 other accounts for security personnel, this is a finding.

Remediation:

Configure the operating system to immediately notify the SA and ISSO (at a minimum) when the threshold for the repository maximum audit record storage capacity is reached.

Uncomment or edit the "action_mail_acct" keyword in "/etc/audit/auditd.conf" and set it to root and any other accounts associated with security personnel.

```
action_mail_acct = root
```

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)

1.139 OL07-00-030360 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all executions of privileged functions.

```
GROUP ID: V-221777
RULE ID: SV-221777r958732
```

Rationale:

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse and identify the risk from insider threats and the advanced persistent threat.

Audit:

Verify the operating system audits the execution of privileged functions using the following command:

```
# grep -iw execve /etc/audit/audit.rules

-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -k setuid
-a always,exit -F arch=b64 -S execve -C uid!=euid -F euid=0 -k setuid
-a always,exit -F arch=b32 -S execve -C gid!=egid -F egid=0 -k setgid
-a always,exit -F arch=b64 -S execve -C gid!=egid -F egid=0 -k setgid
```

If both the "b32" and "b64" audit rules for "SUID" files are not defined, this is a finding.

If both the "b32" and "b64" audit rules for "SGID" files are not defined, this is a finding.

Remediation:

Configure the operating system to audit the execution of privileged functions.

Add or update the following rules in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S execve -C uid!=euid -F euid=0 -k setuid
-a always,exit -F arch=b64 -S execve -C uid!=euid -F euid=0 -k setuid
-a always,exit -F arch=b32 -S execve -C gid!=egid -F egid=0 -k setgid
-a always,exit -F arch=b64 -S execve -C gid!=egid -F egid=0 -k setgid
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

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)

1.140 OL07-00-030370 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the chown, fchown, fchownat, and lchown syscalls.

```
GROUP ID: V-221778
RULE ID: SV-221778r958446
```

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 syscall made by all programs on the system. Therefore, it is very important to use syscall 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 syscalls into one rule whenever possible.

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000458-GPOS-00203, SRG-OS-000474-GPOS-00219

Audit:

Verify the operating system generates audit records upon successful/unsuccessful attempts to use the "chown", "fchown", "fchownat", and "lchown" syscalls.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

```
# grep chown /etc/audit/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
```

If both the “b32” and “b64” audit rules are not defined for the "chown", "fchown", "fchownat", and "lchown" syscalls, this is a finding.

Remediation:

Add or update the following rule 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
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

CCI-000126 Specify the organization-defined event types (subset of the event types defined in AU-2a) along with the frequency of (or situation requiring logging for each identified event type.

- NIST SP 800-53::AU-2 d
- NIST SP 800-53A::AU-2.1 (v)
- NIST SP 800-53 Revision 4::AU-2 d
- NIST SP 800-53 Revision 5::AU-2 c

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

1.141 OL07-00-030410 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the chmod, fchmod, and fchmodat syscalls.

```
GROUP ID: V-221782
RULE ID: SV-221782r991570
```

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 syscall made by all programs on the system. Therefore, it is very important to use syscall 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 syscalls into one rule whenever possible.

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Audit:

Verify the operating system generates audit records upon successful/unsuccessful attempts to use the "chmod", "fchmod", and "fchmodat" syscalls.

Check the file system rules in "/etc/audit/audit.rules" with the following command:

```
# grep chmod /etc/audit/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
```

If both the "b32" and "b64" audit rules are not defined for the "chmod", "fchmod", and "fchmodat" syscalls, this is a finding.

Remediation:

Configure the operating system to generate audit records upon successful/unsuccessful attempts to use the "chmod", "fchmod", and "fchmodat" syscalls.

Add or update the following rule 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
```

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

1.142 OL07-00-030440 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the setxattr, fsetxattr, lsetxattr, removexattr, fremovexattr, and lremovexattr syscalls.

```
GROUP ID: V-221785
RULE ID: SV-221785r991570
```

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 syscall made by all programs on the system. Therefore, it is very important to use syscall 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 syscalls into one rule whenever possible.

Satisfies: SRG-OS-000458-GPOS-00203, SRG-OS-000392-GPOS-00172, SRG-OS-000064-GPOS-00033

Audit:

Verify the operating system generates audit records upon successful/unsuccessful attempts to use the "setxattr", "fsetxattr", "lsetxattr", "removexattr", "fremovexattr", and "lremovexattr" syscalls.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

```
# grep xattr /etc/audit/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
```

If both the "b32" and "b64" audit rules are not defined for the "setxattr", "fsetxattr", "lsetxattr", "removexattr", "fremovexattr", and "lremovexattr" syscalls, this is a finding.

Remediation:

Configure the operating system to generate audit records upon successful/unsuccessful attempts to use the "setxattr", "fsetxattr", "lsetxattr", "removexattr", "fremovexattr", and "lremovexattr" syscalls.

Add or update the following rule in "/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
```

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

1.143 OL07-00-030510 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the creat, open, openat, open_by_handle_at, truncate, and ftruncate syscalls.

```
GROUP ID: V-221792
RULE ID: SV-221792r958446
```

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 syscall made by all programs on the system. Therefore, it is very important to use syscall 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 syscalls into one rule whenever possible.

Satisfies: SRG-OS-000064-GPOS-00033, SRG-OS-000458-GPOS-00203, SRG-OS-000461-GPOS-00205, SRG-OS-000392-GPOS-00172

Audit:

Verify the operating system generates audit records upon successful/unsuccessful attempts to use the "creat", "open", "openat", "open_by_handle_at", "truncate", and "ftruncate" syscalls.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

```
# grep 'open\|truncate\|creat' /etc/audit/audit.rules



-a always,exit -F arch=b32 -S
creat,open,openat,open_by_handle_at,truncate,ftruncate -F exit=-EPERM -F
auid>=1000 -F auid!=unset -k access



-a always,exit -F arch=b32 -S
creat,open,openat,open_by_handle_at,truncate,ftruncate -F exit=-EACCES -F
auid>=1000 -F auid!=unset -k access



-a always,exit -F arch=b64 -S
creat,open,openat,open_by_handle_at,truncate,ftruncate -F exit=-EPERM -F
auid>=1000 -F auid!=unset -k access



-a always,exit -F arch=b64 -S
creat,open,openat,open_by_handle_at,truncate,ftruncate -F exit=-EACCES -F
auid>=1000 -F auid!=unset -k access
```

If both the "b32" and "b64" audit rules are not defined for the "creat", "open", "openat", "open_by_handle_at", "truncate", and "ftruncate" syscalls, this is a finding.

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.

Remediation:

Configure the operating system to generate audit records upon successful/unsuccessful attempts to use the "creat", "open", "openat", "open_by_handle_at", "truncate", and "ftruncate" syscalls.

Add or update the following rules in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S
creat,open,openat,open_by_handle_at,truncate,ftruncate -F exit=-EPERM -F
auid>=1000 -F auid!=unset -k access

-a always,exit -F arch=b32 -S
creat,open,openat,open_by_handle_at,truncate,ftruncate -F exit=-EACCES -F
auid>=1000 -F auid!=unset -k access

-a always,exit -F arch=b64 -S
creat,open,openat,open_by_handle_at,truncate,ftruncate -F exit=-EPERM -F
auid>=1000 -F auid!=unset -k access

-a always,exit -F arch=b64 -S
creat,open,openat,open_by_handle_at,truncate,ftruncate -F exit=-EACCES -F
auid>=1000 -F auid!=unset -k access
```

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

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)

1.144 OL07-00-030560 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the semanage command.

```
GROUP ID: V-221797
RULE ID: SV-221797r958846
```

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.

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "semanage" command occur.

Check the file system rule in "/etc/audit/audit.rules" with the following command:

```
$ sudo grep -w "/usr/sbin/semanage" /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/semanage -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-priv_change
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "semanage" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/semanage -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-priv_change
```

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

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)

1.145 OL07-00-030570 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the setsebool command.

```
GROUP ID: V-221798
RULE ID: SV-221798r958846
```

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.

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "setsebool" command occur.

Check the file system rule in "/etc/audit/audit.rules" with the following command:

```
$ sudo grep -w "/usr/sbin/setsebool" /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/setsebool -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-priv_change
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "setsebool" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/setsebool -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

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)

1.146 OL07-00-030580 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the chcon command.

```
GROUP ID: V-221799
RULE ID: SV-221799r958846
```

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.

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "chcon" command occur.

Check the file system rule in "/etc/audit/audit.rules" with the following command:

```
$ sudo grep -w "/usr/bin/chcon" /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-priv_change
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "chcon" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

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)

1.147 OL07-00-030590 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the setfiles command.

```
GROUP ID: V-221800
RULE ID: SV-221800r958846
```

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.

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000463-GPOS-00207, SRG-OS-000465-GPOS-00209

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "setfiles" command occur.

Check the file system rule in "/etc/audit/audit.rules" with the following command:

```
$ sudo grep -w "/usr/sbin/setfiles" /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/setfiles -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-priv_change
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "setfiles" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/setfiles -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

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)

1.148 OL07-00-030610 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must generate audit records for all unsuccessful account access events.

```
GROUP ID: V-221801
RULE ID: SV-221801r958846
```

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).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Audit:

Verify the operating system generates audit records when unsuccessful account access events occur.

Check the file system rule in "/etc/audit/audit.rules" with the following commands:

```
# grep -i /var/run/faillock /etc/audit/audit.rules

-w /var/run/faillock -p wa -k logins
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when unsuccessful account access events occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-w /var/run/faillock -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 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

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)

1.149 OL07-00-030620 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must generate audit records for all successful account access events.

```
GROUP ID: V-221802
RULE ID: SV-221802r958846
```

Rationale:

Without generating audit records that to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Satisfies: SRG-OS-000392-GPOS-00172, SRG-OS-000470-GPOS-00214, SRG-OS-000473-GPOS-00218

Audit:

Verify the operating system generates audit records when successful account access events occur.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

```
# grep -i /var/log/lastlog /etc/audit/audit.rules

-w /var/log/lastlog -p wa -k logins
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful account access events occur.

Add or update the following rule in "/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.

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

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)

1.150 OL07-00-030630 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the passwd command.

```
GROUP ID: V-221803
RULE ID: SV-221803r958422
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

When a user logs on, the auid is set to the uid of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "passwd" command occur.

Check the file system rule in "/etc/audit/audit.rules" with the following command:

```
$ sudo grep -w "/usr/bin/passwd" /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-passwd
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "passwd" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-passwd
```

The audit daemon must be restarted for the changes to take effect.

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

1.151 OL07-00-030640 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the unix_chkpwd command.

```
GROUP ID: V-221804
RULE ID: SV-221804r958422
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

When a user logs on, the auid is set to the uid of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "unix_chkpwd" command occur.

Check the file system rule in "/etc/audit/audit.rules" with the following command:

```
$ sudo grep -w "/usr/sbin/unix_chkpwd" /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/unix_chkpwd -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-passwd
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "unix_chkpwd" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/unix_chkpwd -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-passwd
```

The audit daemon must be restarted for the changes to take effect.

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

1.152 OL07-00-030650 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the gpasswd command.

```
GROUP ID: V-221805
RULE ID: SV-221805r958422
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

When a user logs on, the auid is set to the uid of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "gpasswd" command occur.

Check the file system rule in "/etc/audit/audit.rules" with the following command:

```
$ sudo grep -w "/usr/bin/gpasswd" /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-passwd
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "gpasswd" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-passwd
```

The audit daemon must be restarted for the changes to take effect.

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

1.153 OL07-00-030660 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the chage command.

```
GROUP ID: V-221806
RULE ID: SV-221806r958422
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

When a user logs on, the auid is set to the uid of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "chage" command occur.

Check the file system rule in "/etc/audit/audit.rules" with the following command:

```
$ sudo grep -w "/usr/bin/chage" /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-passwd
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "chage" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-passwd
```

The audit daemon must be restarted for the changes to take effect.

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

1.154 OL07-00-030670 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the userhelper command.

```
GROUP ID: V-221807
RULE ID: SV-221807r958422
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged password commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

When a user logs on, the auid is set to the uid of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "userhelper" command occur.

Check the file system rule in "/etc/audit/audit.rules" with the following command:

```
$ sudo grep -w "/usr/sbin/userhelper" /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/userhelper -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-passwd
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "userhelper" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/userhelper -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-passwd
```

The audit daemon must be restarted for the changes to take effect.

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

1.155 OL07-00-030680 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the su command.

```
GROUP ID: V-221808
RULE ID: SV-221808r958412
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

When a user logs on, the auid is set to the uid of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "su" command occur.

Check that the following system call is being audited by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w "/usr/bin/su" /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/su -F perm=x -F auid>=1000 -F auid!=unset -k
privileged-priv_change
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "su" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/su -F perm=x -F auid>=1000 -F auid!=unset -k
privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

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

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

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

1.156 OL07-00-030690 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the sudo command.

```
GROUP ID: V-221809
RULE ID: SV-221809r958412
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

When a user logs on, the auid is set to the uid of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "sudo" command occur.

Check that the following system call is being audited by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w "/usr/bin/sudo" /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F auid!=unset -
k privileged-priv_change
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "sudo" command occur.

Add or update 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 privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

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

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

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

1.157 OL07-00-030700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the sudoers file and all files in the /etc/sudoers.d/ directory.

```
GROUP ID: V-221810
RULE ID: SV-221810r958412
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to access the "/etc/sudoers" file and files in the "/etc/sudoers.d/" directory.

Check for modification of the following files being audited by performing the following commands to check the file system rules in "/etc/audit/audit.rules":

```
# grep -i "/etc/sudoers" /etc/audit/audit.rules

-w /etc/sudoers -p wa -k privileged-actions

# grep -i "/etc/sudoers.d/" /etc/audit/audit.rules

-w /etc/sudoers.d/ -p wa -k privileged-actions
```

If the commands do not return output that match the examples, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to access the "/etc/sudoers" file and files in the "/etc/sudoers.d/" directory.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-w /etc/sudoers -p wa -k privileged-actions

-w /etc/sudoers.d/ -p wa -k privileged-actions
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

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

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

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

1.158 OL07-00-030710 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the newgrp command.

```
GROUP ID: V-221811
RULE ID: SV-221811r958412
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

When a user logs on, the auid is set to the uid of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "newgrp" command occur.

Check that the following system call is being audited by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w "/usr/bin/newgrp" /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-priv_change
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "newgrp" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

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

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

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

1.159 OL07-00-030720 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the chsh command.

```
GROUP ID: V-221812
RULE ID: SV-221812r958412
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged access commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

When a user logs on, the auid is set to the uid of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "chsh" command occur.

Check that the following system call is being audited by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w "/usr/bin/chsh" /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F auid!=unset -
k privileged-priv_change
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "chsh" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F auid!=unset -
k privileged-priv_change
```

The audit daemon must be restarted for the changes to take effect.

Additional Information:

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

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

1.160 OL07-00-030740 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the mount command and syscall.

```
GROUP ID: V-221813
RULE ID: SV-221813r958422
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged mount commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

When a user logs on, the auid is set to the uid of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "mount" command and syscall occur.

Check that the following system call is being audited by performing the following series of commands to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w "mount" /etc/audit/audit.rules

-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=unset -k
privileged-mount
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=unset -k
privileged-mount
-a always,exit -F path=/usr/bin/mount -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-mount
```

If both the "b32" and "b64" audit rules are not defined for the "mount" syscall, this is a finding.

If the use of the "mount" command and syscall are not being audited, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "mount" command and syscall occur.

Add or update the following rules in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=unset -k
privileged-mount
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=unset -k
privileged-mount
-a always,exit -F path=/usr/bin/mount -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-mount
```

The audit daemon must be restarted for the changes to take effect.

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

1.161 OL07-00-030750 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the umount command.

```
GROUP ID: V-221814
RULE ID: SV-221814r958422
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged mount commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

When a user logs on, the auid is set to the uid of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "umount" command occur.

Check that the following system call is being audited by performing the following series of commands to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w "/usr/bin/umount" /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/umount -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-mount
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "umount" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/umount -F perm=x -F auid>=1000 -F auid!=unset
-k privileged-mount
```

The audit daemon must be restarted for the changes to take effect.

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

1.162 OL07-00-030760 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the postdrop command.

```
GROUP ID: V-221815
RULE ID: SV-221815r958422
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged postfix commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

When a user logs on, the auid is set to the uid of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "postdrop" command occur.

Check that the following system call is being audited by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w "/usr/sbin/postdrop" /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/postdrop -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-postfix
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "postdrop" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/postdrop -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-postfix
```

The audit daemon must be restarted for the changes to take effect.

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

1.163 OL07-00-030770 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the postqueue command.

```
GROUP ID: V-221816
RULE ID: SV-221816r958422
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged postfix commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

When a user logs on, the auid is set to the uid of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "postqueue" command occur.

Check that the following system call is being audited by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w "/usr/sbin/postqueue" /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/postqueue -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-postfix
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "postqueue" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/postqueue -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-postfix
```

The audit daemon must be restarted for the changes to take effect.

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

1.164 OL07-00-030780 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the ssh-keysign command.

```
GROUP ID: V-221817
RULE ID: SV-221817r958422
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged ssh commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

When a user logs on, the auid is set to the uid of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "ssh-keysign" command occur.

Check that the following system call is being audited by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w "/usr/libexec/openssh/ssh-keysign" /etc/audit/audit.rules

-a always,exit -F path=/usr/libexec/openssh/ssh-keysign -F perm=x -F
auid>=1000 -F auid!=unset -k privileged-ssh
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "ssh-keysign" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/libexec/openssh/ssh-keysign -F perm=x -F
auid>=1000 -F auid!=unset -k privileged-ssh
```

The audit daemon must be restarted for the changes to take effect.

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

1.165 OL07-00-030800 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the crontab command.

```
GROUP ID: V-221818
RULE ID: SV-221818r958422
```

Rationale:

Reconstruction of harmful events or forensic analysis is not possible if audit records do not contain enough information.

At a minimum, the organization must audit the full-text recording of privileged commands. The organization must maintain audit trails in sufficient detail to reconstruct events to determine the cause and impact of compromise.

When a user logs on, the auid is set to the uid of the account that is being authenticated. Daemons are not user sessions and have the loginuid set to -1. The auid representation is an unsigned 32-bit integer, which equals 4294967295. The audit system interprets -1, 4294967295, and "unset" in the same way.

Satisfies: SRG-OS-000042-GPOS-00020, SRG-OS-000392-GPOS-00172, SRG-OS-000471-GPOS-00215

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "crontab" command occur.

Check that the following system call is being audited by performing the following command to check the file system rules in "/etc/audit/audit.rules":

```
$ sudo grep -w "/usr/bin/crontab" /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-cron
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "crontab" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F
auid!=unset -k privileged-cron
```

The audit daemon must be restarted for the changes to take effect.

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

1.166 OL07-00-030805 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

OL 7 must audit any script or executable called by cron as root or by any privileged user.

```
GROUP ID: V-274875
RULE ID: SV-274875r1101859
```

Rationale:

Any script or executable called by cron as root or by any privileged user must be owned by that user and must have the permissions 755 or more restrictive and should have no extended rights that allow any nonprivileged user to modify the script or executable.

Audit:

Verify that OL 7 is configured to audit the execution of any system call made by cron as root or as any privileged user.

```
$ sudo auditctl -l | grep /etc/cron.d

-w /etc/cron.d -p wa -k cronjobs
$ sudo auditctl -l | grep /var/spool/cron

-w /var/spool/cron -p wa -k cronjobs
```

If either of these commands do not return the expected output, or the lines are commented out, this is a finding.

Remediation:

Configure OL 7 to audit the execution of any system call made by cron as root or as any privileged user.

Add or update the following file system rules to "/etc/audit/rules.d/audit.rules":

```
auditctl -w /etc/cron.d/ -p wa -k cronjobs
auditctl -w /var/spool/cron/ -p wa -k cronjobs
```

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

1.167 OL07-00-030810 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the pam_timestamp_check command.

```
GROUP ID: V-221819
RULE ID: SV-221819r991579
```

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.

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.

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "pam_timestamp_check" command occur.

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
$ sudo grep -w "/usr/sbin/pam_timestamp_check" /etc/audit/audit.rules

-a always,exit -F path=/usr/sbin/pam_timestamp_check -F perm=x -F auid>=1000
-F auid!=unset -k privileged-pam
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "pam_timestamp_check" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/sbin/pam_timestamp_check -F perm=x -F auid>=1000
-F auid!=unset -k privileged-pam
```

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

1.168 OL07-00-030819 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the create_module syscall.

```
GROUP ID: V-221820
RULE ID: SV-221820r991580
```

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).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "create_module" syscall occur.

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
$ sudo grep -w "create_module" /etc/audit/audit.rules

-a always,exit -F arch=b32 -S create_module -F auid>=1000 -F auid!=unset -k
module-change

-a always,exit -F arch=b64 -S create_module -F auid>=1000 -F auid!=unset -k
module-change
```

If both the "b32" and "b64" audit rules are not defined for "create_module" syscall, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "create_module" syscall occur.

Add or update the following rules in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S create_module -F auid>=1000 -F auid!=unset -k
module-change

-a always,exit -F arch=b64 -S create_module -F auid>=1000 -F auid!=unset -k
module-change
```

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

1.169 OL07-00-030820 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the init_module and finit_module syscalls.

```
GROUP ID: V-221821
RULE ID: SV-221821r991580
```

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).

The system call rules are loaded into a matching engine that intercepts each syscall made by all programs on the system. Therefore, it is very important to use syscall 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 syscalls into one rule whenever possible.

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Audit:

Verify the operating system generates audit records upon successful/unsuccessful attempts to use the "init_module" and "finit_module" syscalls.

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the line appropriate for the system architecture must be present.

```
$ sudo grep init_module /etc/audit/audit.rules

-a always,exit -F arch=b32 -S init_module,finit_module -F auid>=1000 -F
auid!=unset -k modulechange

-a always,exit -F arch=b64 -S init_module,finit_module -F auid>=1000 -F
auid!=unset -k modulechange
```

If there are no audit rules defined for "init_module" and "finit_module", this is a finding.

Remediation:

Configure the operating system to generate audit records upon successful/unsuccessful attempts to use the "init_module" and "finit_module" syscalls.

Add or update the following rules in "/etc/audit/rules.d/audit.rules":

Note: The rules are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be configured.

```
-a always,exit -F arch=b32 -S init_module,finit_module -F auid>=1000 -F
auid!=unset -k modulechange

-a always,exit -F arch=b64 -S init_module,finit_module -F auid>=1000 -F
auid!=unset -k modulechange
```

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

1.170 OL07-00-030830 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the delete_module syscall.

```
GROUP ID: V-221823
RULE ID: SV-221823r991580
```

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).

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "delete_module" syscall occur.

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

Note: The output lines of the command are duplicated to cover both 32-bit and 64-bit architectures. Only the line appropriate for the system architecture must be present.

```
$ sudo grep -w "delete_module" /etc/audit/audit.rules

-a always,exit -F arch=b32 -S delete_module -F auid>=1000 -F auid!=unset -k
module-change

-a always,exit -F arch=b64 -S delete_module -F auid>=1000 -F auid!=unset -k
module-change
```

If there are no audit rules defined for "delete_module", this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "delete_module" syscall occur.

Add or update the following rules in "/etc/audit/rules.d/audit.rules":

Note: The rules are duplicated to cover both 32-bit and 64-bit architectures. Only the lines appropriate for the system architecture must be configured.

```
-a always,exit -F arch=b32 -S delete_module -F auid>=1000 -F auid!=unset -k
module-change

-a always,exit -F arch=b64 -S delete_module -F auid>=1000 -F auid!=unset -k
module-change
```

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

1.171 OL07-00-030840 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the kmod command.

```
GROUP ID: V-221824
RULE ID: SV-221824r991580
```

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.

Satisfies: SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Audit:

Verify the operating system generates audit records when successful/unsuccessful attempts to use the "kmod" command occur.

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
$ sudo grep "/usr/bin/kmod" /etc/audit/audit.rules

-a always,exit -F path=/usr/bin/kmod -F perm=x -F auid>=1000 -F auid!=unset -
k modules
```

If the command does not return any output, this is a finding.

Remediation:

Configure the operating system to generate audit records when successful/unsuccessful attempts to use the "kmod" command occur.

Add or update the following rule in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F path=/usr/bin/kmod -F perm=x -F auid>=1000 -F auid!=unset -
k modules
```

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

1.172 OL07-00-030870 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd.

```
GROUP ID: V-221825
RULE ID: SV-221825r958368
```

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).

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000303-GPOS-00120, SRG-OS-000476-GPOS-00221

Audit:

Verify the operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
# grep /etc/passwd /etc/audit/audit.rules

-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 the operating system to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/passwd".

Add or update the following rule "/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-000018 Automatically audit account creation actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

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

CCI-001403 Automatically audit account modification actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-001404 Automatically audit account disabling actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

CCI-001405 Automatically audit account removal actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

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)

1.173 OL07-00-030871 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/group.

```
GROUP ID: V-221826
RULE ID: SV-221826r958368
```

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).

Audit:

Verify the operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/group".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
# grep /etc/group /etc/audit/audit.rules

-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 the operating system to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/group".

Add or update the following rule in "/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 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

1.174 OL07-00-030872 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/gshadow.

```
GROUP ID: V-221827
RULE ID: SV-221827r958368
```

Rationale:

Without generating audit specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/gshadow".

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
# grep /etc/gshadow /etc/audit/audit.rules

-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 the operating system to generate audit records for all account creations, modifications, disabling, and termination events that affect "/etc/gshadow".

Add or update the following rule in "/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 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

1.175 OL07-00-030873 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow.

```
GROUP ID: V-221828
RULE ID: SV-221828r958368
```

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).

Audit:

Verify the operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow.

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
# grep /etc/shadow /etc/audit/audit.rules

-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 the operating system 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 in "/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 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

1.176 OL07-00-030874 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/security/opasswd.

```
GROUP ID: V-221829
RULE ID: SV-221829r958368
```

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).

Audit:

Verify the operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/security/opasswd.

Check the auditing rules in "/etc/audit/audit.rules" with the following command:

```
# grep /etc/security/opasswd /etc/audit/audit.rules

-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 the operating system 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 in "/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:

```
# systemctl restart auditd
```

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53 Revision 5::AC-2 (4)

1.177 OL07-00-030910 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must audit all uses of the unlink, unlinkat, rename, renameat, and rmdir syscalls.

```
GROUP ID: V-221833
RULE ID: SV-221833r991575
```

Rationale:

If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.

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 syscall made by all programs on the system. Therefore, it is very important to use syscall 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 syscalls into one rule whenever possible.

Satisfies: SRG-OS-000466-GPOS-00210, SRG-OS-000467-GPOS-00211, SRG-OS-000468-GPOS-00212, SRG-OS-000392-GPOS-00172

Audit:

Verify the operating system generates audit records upon successful/unsuccessful attempts to use the "unlink", "unlinkat", "rename", "renameat", and "rmdir" syscalls.

Check the file system rules in "/etc/audit/audit.rules" with the following commands:

```
# grep 'unlink\|rename\|rmdir' /etc/audit/audit.rules

-a always,exit -F arch=b32 -S unlink,unlinkat,rename,renameat,rmdir -F
auid>=1000 -F auid!=unset -k delete

-a always,exit -F arch=b64 -S unlink,unlinkat,rename,renameat,rmdir -F
auid>=1000 -F auid!=unset -k delete
```

If both the "b32" and "b64" audit rules are not defined for the "unlink", "unlinkat", "rename", "renameat", and "rmdir" syscalls, this is a finding.

Remediation:

Configure the operating system to generate audit records upon successful/unsuccessful attempts to use the "unlink", "unlinkat", "rename", "renameat", and "rmdir" syscalls.

Add the following rules in "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S unlink,unlinkat,rename,renameat,rmdir -F
auid>=1000 -F auid!=unset -k delete

-a always,exit -F arch=b64 -S unlink,unlinkat,rename,renameat,rmdir -F
auid>=1000 -F auid!=unset -k delete
```

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

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)

1.178 OL07-00-031000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must send rsyslog output to a log aggregation server.

```
GROUP ID: V-221835
RULE ID: SV-221835r991589
```

Rationale:

Sending rsyslog output to another system ensures that the logs cannot be removed or modified in the event that the system is compromised or has a hardware failure.

Audit:

Verify "rsyslog" is configured to send all messages to a log aggregation server.

Check the configuration of "rsyslog" with the following command:

Note: If another logging package is used, substitute the utility configuration file for "/etc/rsyslog.conf".

```
# grep @ /etc/rsyslog.conf /etc/rsyslog.d/*.conf

*.* @@[logaggregationserver.example.mil]:[port]
```

If there are no lines in the "/etc/rsyslog.conf" or "/etc/rsyslog.d/*.conf" files that contain the "@" or "@@" symbol(s), and the lines with the correct symbol(s) to send output to another system do not cover all "rsyslog" output, ask the system administrator to indicate how the audit logs are offloaded to a different system or media.

If the lines are commented out or there is no evidence that the audit logs are being sent to another system, this is a finding.

Remediation:

Modify the "/etc/rsyslog.conf" or an "/etc/rsyslog.d/*.conf" file to contain a configuration line to send all "rsyslog" output to a log aggregation server:

For UDP:

```
*.* @[logaggregationserver.example.mil]:[port]
```

For TCP:

```
*.* @@[logaggregationserver.example.mil]:[port]
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.179 OL07-00-031010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system 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-221836
RULE ID: SV-221836r991589
```

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 in to 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 ISSO.

Audit:

Verify that the system is not accepting "rsyslog" messages from other systems unless it is documented as a log aggregation server.

Check the configuration of "rsyslog" with the following command:

```
# grep imtcp /etc/rsyslog.conf

$ModLoad imtcp

# grep imudp /etc/rsyslog.conf

$ModLoad imudp

# grep imrelp /etc/rsyslog.conf

$ModLoad imrelp
```

If any of the above modules are being loaded in the "/etc/rsyslog.conf" file, 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:

Modify the "/etc/rsyslog.conf" file to remove the "ModLoad imtcp", "ModLoad imudp", and "ModLoad imrelp" configuration lines, or document the system as being used for log aggregation.

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.180 OL07-00-032000 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must use a virus scan program.

```
GROUP ID: V-221837
RULE ID: SV-221837r991589
```

Rationale:

Virus scanning software can be used to protect a system from penetration from computer viruses and to limit their spread through intermediate systems.

The virus scanning software should be configured to perform scans dynamically on accessed files. If this capability is not available, the system must be configured to scan, at a minimum, all altered files on the system on a daily basis.

If the system processes inbound SMTP mail, the virus scanner must be configured to scan all received mail.

Audit:

Verify an anti-virus solution is installed on the system. The anti-virus solution may be bundled with an approved host-based security solution.

If there is no anti-virus solution installed on the system, this is a finding.

Remediation:

Install an antivirus solution on the system.

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.181 OL07-00-040000 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Oracle Linux operating system must limit the number of concurrent sessions to 10 for all accounts and/or account types.

```
GROUP ID: V-221838
RULE ID: SV-221838r958398
```

Rationale:

Operating system management includes the ability to control the number of users and user sessions that utilize an operating system. Limiting the number of allowed users and sessions per user is helpful in reducing the risks related to DoS attacks.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based on mission needs and the operational environment for each system.

Audit:

Verify the operating system limits the number of concurrent sessions to 10 for all accounts and/or account types by issuing the following command:

```
# grep "maxlogins" /etc/security/limits.conf /etc/security/limits.d/*.conf
* hard maxlogins 10
```

This can be set as a global domain (with the * wildcard) but may be set differently for multiple domains.

If the "maxlogins" item is missing, commented out, or the value is not set to "10" or less for all domains that have the "maxlogins" item assigned, this is a finding.

Remediation:

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

Add the following line to the top of the /etc/security/limits.conf or in a ".conf" file defined in /etc/security/limits.d/ :

```
* hard maxlogins 10
```

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 800-53A::AC-10.1 (ii)
- NIST SP 800-53 Revision 4::AC-10
- NIST SP 800-53 Revision 5::AC-10

1.182 OL07-00-040100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the Ports, Protocols, and Services Management Component Local Service Assessment (PPSM CLSA) and vulnerability assessments.

```
GROUP ID: V-221839
RULE ID: SV-221839r958480
```

Rationale:

In order to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

Operating systems are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., VPN and IPS); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the operating system must support the organizational requirements, providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality of life issues.

Satisfies: SRG-OS-000096-GPOS-00050, SRG-OS-000297-GPOS-00115

Audit:

Inspect the firewall configuration and running services to verify that it is configured to prohibit or restrict the use of functions, ports, protocols, and/or services that are unnecessary or prohibited.

Check which services are currently active with the following command:

```
# firewall-cmd --list-all
public (default, active)
interfaces: enp0s3
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 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 ports, protocols, or services 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.

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 800-53A::CM-7.1 (iii)
- NIST SP 800-53 Revision 4::CM-7 b
- NIST SP 800-53 Revision 5::CM-7 b

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)

1.183 OL07-00-040110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux 7 operating system must implement DoD-approved encryption to protect the confidentiality of SSH connections.

```
GROUP ID: V-221840
RULE ID: SV-221840r958408
```

Rationale:

Unapproved mechanisms for authentication to the cryptographic module are not verified, and therefore cannot be relied upon to provide confidentiality or integrity, resulting in the compromise of DoD data.

Operating systems using encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

FIPS 140-2 is the current standard for validating 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.

The system will attempt to use the first cipher presented by the client that matches the server list. Listing the values "strongest to weakest" is a method to ensure the use of the strongest cipher available to secure the SSH connection.

Satisfies: SRG-OS-000033-GPOS-00014, SRG-OS-000120-GPOS-00061, SRG-OS-000125-GPOS-00065, SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173,SRG-OS-000394-GPOS-00174

Audit:

Verify the operating system uses mechanisms that meet the requirements of applicable federal laws, Executive orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

The location of the "sshd_config" file may vary if a different daemon is in use.

Inspect the "Ciphers" configuration with the following command:

```
# grep -i ciphers /etc/ssh/sshd_config
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
```

If any ciphers other than "aes256-ctr", "aes192-ctr", or "aes128-ctr" are listed, the order differs from the example above, the "Ciphers" keyword is missing, or the returned line is commented out, this is a finding.

Remediation:

Configure SSH to use FIPS 140-2 approved cryptographic algorithms.

Add the following line (or modify the line to have the required value) to the "/etc/ssh/sshd_config" file (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor).

```
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
```

The SSH service must be restarted for 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 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

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 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

CCI-000877 Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53::MA-4 c
- NIST SP 800-53A::MA-4.1 (iv)
- NIST SP 800-53 Revision 4::MA-4 c
- NIST SP 800-53 Revision 5::MA-4 c

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)

1.184 OL07-00-040160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that all network connections associated with a communication session are terminated at the end of the session or after 15 minutes of inactivity from the user at a command prompt, except to fulfill documented and validated mission requirements.

```
GROUP ID: V-221841
RULE ID: SV-221841r1014784
```

Rationale:

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level and de-allocating networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. This does not mean that the operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Audit:

Verify the operating system terminates all network connections associated with a communications session at the end of the session or based on inactivity.

Check the value of the system inactivity timeout with the following command:

```
$ sudo grep -irw tmout /etc/profile /etc/bashrc /etc/profile.d

etc/profile.d/tmout.sh:declare -xr TMOUT=600
```

If conflicting results are returned, this is a finding.

If "TMOUT" is not set to "600" or less to enforce session termination after inactivity, this is a finding.

Remediation:

Configure the operating system to terminate all network connections associated with a communications session at the end of the session or after a period of inactivity.

Create a script to enforce the inactivity timeout (for example /etc/profile.d/tmout.sh) such as:

```
#!/bin/bash

declare -xr TMOUT=600
```

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 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

1.185 OL07-00-040170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-221842
RULE ID: SV-221842r958390
```

Rationale:

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

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

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

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

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

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

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

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

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

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

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007 , SRG-OS-000228-GPOS-00088

Audit:

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

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

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

banner /etc/issue
```

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

If the line is commented out, this is a finding.

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

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

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

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

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

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

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

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

If the system does not display a graphical logon banner or the banner does not match the Standard Mandatory DoD Notice and Consent Banner, this is a finding.

If the text in the file does not match the Standard Mandatory DoD Notice and Consent Banner, this is a finding.

Remediation:

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

Edit the "/etc/ssh/sshd_config" file to uncomment the banner keyword and configure it to point to a file that will contain the logon banner (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor). An example configuration line is:

```
banner /etc/issue
```

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

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

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

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

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

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

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

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

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

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

1.186 OL07-00-040180 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) authentication communications.

```
GROUP ID: V-221843
RULE ID: SV-221843r991554
```

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Audit:

If LDAP is not being utilized, this requirement is Not Applicable.

Verify the operating system implements cryptography to protect the integrity of remote LDAP authentication sessions.

To determine if LDAP is being used for authentication, use the following command:

```
 # systemctl status sssd.service
 sssd.service - System Security Services Daemon
 Loaded: loaded (/usr/lib/systemd/system/sssd.service; enabled; vendor
preset: disabled)
 Active: active (running) since Wed 2018-06-27 10:58:11 EST; 1h 50min ago
```

If the "sssd.service" is "active", then LDAP is being used.

Determine the "id_provider" the LDAP is currently using:

```
 # grep -ir id_provider /etc/sssd/sssd.conf /etc/sssd/conf.d/*.conf
 id_provider = ad
```

If "id_provider" is set to "ad", this is Not Applicable.

Ensure LDAP is configured to use TLS, by using the following command:

```
 # grep -ir start_tls /etc/sssd/sssd.conf /etc/sssd/conf.d/*.conf
 ldap_id_use_start_tls = true
```

If the "ldap_id_use_start_tls" option is not "true", this is a finding.

Remediation:

Configure the operating system to implement cryptography to protect the integrity of LDAP authentication sessions.

Add or modify the following line in "/etc/sssd/sssd.conf":

```
ldap_id_use_start_tls = true
```

Additional Information:

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

1.187 OL07-00-040190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications.

```
GROUP ID: V-221844
RULE ID: SV-221844r991554
```

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Audit:

If LDAP is not being utilized, this requirement is Not Applicable.

Verify the operating system implements cryptography to protect the integrity of remote LDAP access sessions.

To determine if LDAP is being used for authentication, use the following command:

```
 # systemctl status sssd.service
 sssd.service - System Security Services Daemon
 Loaded: loaded (/usr/lib/systemd/system/sssd.service; enabled; vendor
preset: disabled)
 Active: active (running) since Wed 2018-06-27 10:58:11 EST; 1h 50min ago
```

If the "sssd.service" is "active", then LDAP is being used.

Determine the "id_provider" the LDAP is currently using:

```
 # grep -ir id_provider /etc/sssd/sssd.conf /etc/sssd/conf.d/*.conf
 id_provider = ad
```

If "id_provider" is set to "ad", this is Not Applicable.

Verify the sssd service is configured to require the use of certificates:

```
 # grep -ir tls_reqcert /etc/sssd/sssd.conf /etc/sssd/conf.d/*.conf
 ldap_tls_reqcert = demand
```

If the "ldap_tls_reqcert" setting is missing, commented out, or does not exist, this is a finding.

If the "ldap_tls_reqcert" setting is not set to "demand" or "hard", this is a finding.

Remediation:

Configure the operating system to implement cryptography to protect the integrity of LDAP remote access sessions.

Add or modify the following line in "/etc/sssd/sssd.conf":

```
ldap_tls_reqcert = demand
```

Additional Information:

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

1.188 OL07-00-040200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must implement cryptography to protect the integrity of Lightweight Directory Access Protocol (LDAP) communications.

```
GROUP ID: V-221845
RULE ID: SV-221845r991554
```

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the key used to generate the hash.

Audit:

If LDAP is not being utilized, this requirement is Not Applicable.

Verify the operating system implements cryptography to protect the integrity of remote LDAP access sessions.

To determine if LDAP is being used for authentication, use the following command:

```
 # systemctl status sssd.service
 sssd.service - System Security Services Daemon
 Loaded: loaded (/usr/lib/systemd/system/sssd.service; enabled; vendor
preset: disabled)
 Active: active (running) since Wed 2018-06-27 10:58:11 EST; 1h 50min ago
```

If the "sssd.service" is "active", then LDAP is being used.

Determine the "id_provider" that the LDAP is currently using:

```
 # grep -ir id_provider /etc/sssd/sssd.conf /etc/sssd/conf.d/*.conf
 id_provider = ad
```

If "id_provider" is set to "ad", this is Not Applicable.

Check the path to the X.509 certificate for peer authentication with the following command:

```
 # grep -ir tls_cacert /etc/sssd/sssd.conf /etc/sssd/conf.d/*.conf
 ldap_tls_cacert = /etc/pki/tls/certs/ca-bundle.crt
```

Verify the "ldap_tls_cacert" option points to a file that contains the trusted CA certificate.

If this file does not exist, or the option is commented out or missing, this is a finding.

Remediation:

Configure the operating system to implement cryptography to protect the integrity of LDAP remote access sessions.

Add or modify the following line in "/etc/sssd/sssd.conf":

```
ldap_tls_cacert = /etc/pki/tls/certs/ca-bundle.crt
```

Additional Information:

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

1.189 OL07-00-040201 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must implement virtual address space randomization.

```
GROUP ID: V-221846
RULE ID: SV-221846r958928
```

Rationale:

Address space layout randomization (ASLR) makes it more difficult for an attacker to predict the location of attack code introduced into a process's address space during an attempt at exploitation. Additionally, ASLR also 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.

Audit:

Verify the operating system implements virtual address space randomization.

```
 # grep -r kernel.randomize_va_space /run/sysctl.d/* /etc/sysctl.d/*
/usr/local/lib/sysctl.d/* /usr/lib/sysctl.d/* /lib/sysctl.d/*
/etc/sysctl.conf 2> /dev/null
 kernel.randomize_va_space = 2
```

If "kernel.randomize_va_space" is not configured in the /etc/sysctl.conf file or in any of the other sysctl.d directories, is commented out or does not have a value of "2", this is a finding.

Check that the operating system implements virtual address space randomization with the following command:

```
 # /sbin/sysctl -a | grep kernel.randomize_va_space
 kernel.randomize_va_space = 2
```

If "kernel.randomize_va_space" does not have a value of "2", this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure the operating system implement virtual address space randomization.

Set the system to the required kernel parameter by adding the following line to "/etc/sysctl.conf" or a config file in the /etc/sysctl.d/ directory (or modify the line to have the required value):

```
kernel.randomize_va_space = 2
```

Issue the following command to make the changes take effect:

```
# sysctl --system
```

Additional Information:

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

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

1.190 OL07-00-040300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that all networked systems have SSH installed.

```
GROUP ID: V-221847
RULE ID: SV-221847r958908
```

Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Audit:

Check to see if sshd is installed with the following command:

```
# yum list installed \*ssh\*
libssh2.x86_64 1.4.3-8.el7 @anaconda/7.1
openssh.x86_64 6.6.1p1-11.el7 @anaconda/7.1
openssh-server.x86_64 6.6.1p1-11.el7 @anaconda/7.1
```

If the "SSH server" package is not installed, this is a finding.

Remediation:

Install SSH packages onto the host with the following commands:

```
# yum install openssh-server.x86_64
```

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-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)

1.191 OL07-00-040310 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that all networked systems use SSH for confidentiality and integrity of transmitted and received information as well as information during preparation for transmission.

```
GROUP ID: V-221848
RULE ID: SV-221848r958908
```

Rationale:

Without protection of the transmitted information, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read or altered.

This requirement applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, and facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of organizational information can be accomplished by physical means (e.g., employing physical distribution systems) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa.

Satisfies: SRG-OS-000423-GPOS-00187, SRG-OS-000424-GPOS-00188, SRG-OS-000425-GPOS-00189, SRG-OS-000426-GPOS-00190

Audit:

Verify SSH is loaded and active with the following command:

```
# systemctl status sshd
sshd.service - OpenSSH server daemon
Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled)
Active: active (running) since Tue 2015-11-17 15:17:22 EST; 4 weeks 0 days
ago
Main PID: 1348 (sshd)
CGroup: /system.slice/sshd.service
1053 /usr/sbin/sshd -D
```

If "sshd" does not show a status of "active" and "running", this is a finding.

Remediation:

Configure the SSH service to automatically start after reboot with the following command:

```
# systemctl enable sshd.service
```

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

1.192 OL07-00-040320 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that all network connections associated with SSH traffic are terminated after 10 minutes of becoming unresponsive.

```
GROUP ID: V-221849
RULE ID: SV-221849r970703
```

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.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109

Audit:

Verify the SSH server automatically terminates a user session after the SSH client has been unresponsive for 10 minutes.

Check for the value of the "ClientAliveInterval" keyword with the following command:

```
 # grep -iw clientaliveinterval /etc/ssh/sshd_config

 ClientAliveInterval 600
```

If "ClientAliveInterval" is not configured, is commented out, or has a value of "0", this is a finding.

If "ClientAliveInterval" has a value that is greater than "600" and is not documented with the information system security officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Note: This setting must be applied in conjunction with OL07-00-040340 to function correctly.

Configure the SSH server to terminate a user session automatically after the SSH client has become unresponsive.

Add the following line (or modify the line to have the required value) to the "/etc/ssh/sshd_config" file (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor):

```
ClientAliveInterval 600
```

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

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 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

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

1.193 OL07-00-040330 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that the SSH daemon does not allow authentication using RSA rhosts authentication.

```
GROUP ID: V-221850
RULE ID: SV-221850r991589
```

Rationale:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Audit:

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

```
# cat /etc/oracle-release
```

If the release is 7.4 or newer this requirement is Not Applicable.

Verify the SSH daemon does not allow authentication using RSA rhosts authentication.

To determine how the SSH daemon's "RhostsRSAAuthentication" option is set, run the following command:

```
# grep RhostsRSAAuthentication /etc/ssh/sshd_config
RhostsRSAAuthentication no
```

If the value is returned as "yes", the returned line is commented out, or no output is returned, this is a finding.

Remediation:

Configure the SSH daemon to not allow authentication using RSA rhosts authentication.

Add the following line in "/etc/ssh/sshd_config", or uncomment the line and set the value to "no":

```
RhostsRSAAuthentication no
```

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

1.194 OL07-00-040340 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that all network connections associated with SSH traffic terminate after becoming unresponsive.

```
GROUP ID: V-221851
RULE ID: SV-221851r970703
```

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.

Satisfies: SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109

Audit:

Verify the SSH server automatically terminates a user session after the SSH client has become unresponsive.

Check for the value of the "ClientAliveCountMax" keyword with the following command:

```
 # grep -i clientalivecount /etc/ssh/sshd_config
 ClientAliveCountMax 0
```

If "ClientAliveCountMax" is not set to "0", this is a finding.

Remediation:

Note: This setting must be applied in conjunction with OL07-00-040320 to function correctly.

Configure the SSH server to terminate a user session automatically after the SSH client has become unresponsive.

Add the following line (or modify the line to have the required value) to the "/etc/ssh/sshd_config" file (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor):

```
ClientAliveCountMax 0
```

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

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 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

1.195 OL07-00-040350 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that the SSH daemon does not allow authentication using rhosts authentication.

```
GROUP ID: V-221852
RULE ID: SV-221852r991589
```

Rationale:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Audit:

Verify the SSH daemon does not allow authentication using known hosts authentication.

To determine how the SSH daemon's "IgnoreRhosts" option is set, run the following command:

```
# grep -i IgnoreRhosts /etc/ssh/sshd_config

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 authentication using known hosts authentication.

Add the following line in "/etc/ssh/sshd_config", or uncomment the line and set the value to "yes":

```
IgnoreRhosts yes
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.196 OL07-00-040360 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must display the date and time of the last successful account logon upon an SSH logon.

```
GROUP ID: V-221853
RULE ID: SV-221853r991589
```

Rationale:

Providing users with feedback on when account accesses via SSH last occurred facilitates user recognition and reporting of unauthorized account use.

Audit:

Verify SSH provides users with feedback on when account accesses last occurred.

Check that "PrintLastLog" keyword in the sshd daemon configuration file is used and set to "yes" with the following command:

```
# grep -i printlastlog /etc/ssh/sshd_config
PrintLastLog yes
```

If the "PrintLastLog" keyword is set to "no", is missing, or is commented out, this is a finding.

Remediation:

Configure SSH to provide users with feedback on when account accesses last occurred by setting the required configuration options in "/etc/pam.d/sshd" or in the "sshd_config" file used by the system ("/etc/ssh/sshd_config" will be used in the example) (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor).

Modify the "PrintLastLog" line in "/etc/ssh/sshd_config" to match the following:

```
PrintLastLog yes
```

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

Additional Information:

CCI-000052 Notify the user, upon successful logon (access) to the system, of the date and time of the last logon (access).

- NIST SP 800-53::AC-9
- NIST SP 800-53A::AC-9.1
- NIST SP 800-53 Revision 4::AC-9
- NIST SP 800-53 Revision 5::AC-9

1.197 OL07-00-040370 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must not permit direct logons to the root account using remote access via SSH.

```
GROUP ID: V-221854
RULE ID: SV-221854r991589
```

Rationale:

Even though the communications channel may be encrypted, an additional layer of security is gained by extending the policy of not logging on directly as root. In addition, logging on with a user-specific account provides individual accountability of actions performed on the system.

Audit:

Verify remote access using SSH prevents users from logging on directly as root.

Check that SSH prevents users from logging on directly as root with the following command:

```
# grep -i permitrootlogin /etc/ssh/sshd_config
PermitRootLogin no
```

If the "PermitRootLogin" keyword is set to "yes", is missing, or is commented out, this is a finding.

Remediation:

Configure SSH to stop users from logging on remotely as the root user.

Edit the appropriate "/etc/ssh/sshd_config" file to uncomment or add the line for the "PermitRootLogin" keyword and set its value to "no" (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):

```
PermitRootLogin no
```

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

1.198 OL07-00-040380 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that the SSH daemon does not allow authentication using known hosts authentication.

```
GROUP ID: V-221855
RULE ID: SV-221855r991589
```

Rationale:

Configuring this setting for the SSH daemon provides additional assurance that remote logon via SSH will require a password, even in the event of misconfiguration elsewhere.

Audit:

Verify the SSH daemon does not allow authentication using known hosts authentication.

To determine how the SSH daemon's "IgnoreUserKnownHosts" option is set, run the following command:

```
# grep -i IgnoreUserKnownHosts /etc/ssh/sshd_config

IgnoreUserKnownHosts yes
```

If the value is returned as "no", the returned line is commented out, or no output is returned, this is a finding.

Remediation:

Configure the SSH daemon to not allow authentication using known hosts authentication.

Add the following line in "/etc/ssh/sshd_config", or uncomment the line and set the value to "yes":

```
IgnoreUserKnownHosts yes
```

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

1.199 OL07-00-040390 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must be configured so that the SSH daemon is configured to only use the SSHv2 protocol.

```
GROUP ID: V-221856
RULE ID: SV-221856r987796
```

Rationale:

SSHv1 is an insecure implementation of the SSH protocol and has many well-known vulnerability exploits. Exploits of the SSH daemon could provide immediate root access to the system.

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

Audit:

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

```
# cat /etc/oracle-release
```

If the release is 7.4 or newer this requirement is Not Applicable.

Verify the SSH daemon is configured to only use the SSHv2 protocol.

Check that the SSH daemon is configured to only use the SSHv2 protocol with the following command:

```
# grep -i protocol /etc/ssh/sshd_config
Protocol 2
#Protocol 1,2
```

If any protocol line other than "Protocol 2" is uncommented, this is a finding.

Remediation:

Remove all Protocol lines that reference version "1" in "/etc/ssh/sshd_config" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor). The "Protocol" line must be as follows:

```
Protocol 2
```

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

Additional Information:

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

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

1.200 OL07-00-040400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that the SSH daemon is configured to only use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hash algorithms.

```
GROUP ID: V-221857
RULE ID: SV-221857r991554
```

Rationale:

DoD information systems are required to use FIPS 140-2 approved cryptographic hash functions. The only SSHv2 hash algorithm meeting this requirement is SHA.

The system will attempt to use the first hash presented by the client that matches the server list. Listing the values "strongest to weakest" is a method to ensure the use of the strongest hash available to secure the SSH connection.

Audit:

Verify the SSH daemon is configured to only use MACs employing FIPS 140-2-approved hashes.

Note: If OL07-00-021350 is a finding, this is automatically a finding, as the system cannot implement FIPS 140-2-approved cryptographic algorithms and hashes.

Check that the SSH daemon is configured to only use MACs employing FIPS 140-2-approved hashes with the following command:

```
# grep -i macs /etc/ssh/sshd_config
MACs hmac-sha2-512,hmac-sha2-256
```

If any ciphers other than "hmac-sha2-512" or "hmac-sha2-256" are listed, the order differs from the example above, they are missing, or the returned line is commented out, this is a finding.

Remediation:

Edit the "/etc/ssh/sshd_config" file to uncomment or add the line for the "MACs" keyword and set its value to "hmac-sha2-512" and/or "hmac-sha2-256" (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):

```
MACs hmac-sha2-512,hmac-sha2-256
```

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

Additional Information:

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

1.201 OL07-00-040410 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that the SSH public host key files have mode 0644 or less permissive.

```
GROUP ID: V-221858
RULE ID: SV-221858r991589
```

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 mode 0644 or less permissive.

Note: SSH public key files may be found in other directories on the system depending on the installation.

The following command will find all SSH public key files on the system:

```
# find /etc/ssh -name '*.pub' -exec ls -lL {} \;

-rw-r--r-- 1 root root 618 Nov 28 06:43 ssh_host_dsa_key.pub
-rw-r--r-- 1 root root 347 Nov 28 06:43 ssh_host_key.pub
-rw-r--r-- 1 root root 238 Nov 28 06:43 ssh_host_rsa_key.pub
```

If any file has a mode more permissive than 0644, this is a finding.

Remediation:

Note: SSH public key files may be found in other directories on the system depending on the installation.

Change the mode of public host key files under "/etc/ssh" to "0644" with the following command:

```
# chmod 0644 /etc/ssh/*.key.pub
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.202 OL07-00-040420 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so the SSH private host key files have mode 0640 or less permissive.

```
GROUP ID: V-221859
RULE ID: SV-221859r991589
```

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 mode 0640 or less permissive.

The following command will find all SSH private key files on the system and list their modes:

```
 # find / -name '*ssh_host*key' | xargs ls -lL

 -rw-r----- 1 root ssh_keys 112 Apr 1 11:59 ssh_host_dsa_key
 -rw-r----- 1 root ssh_keys 202 Apr 1 11:59 ssh_host_key
 -rw-r----- 1 root ssh_keys 352 Apr 1 11:59 ssh_host_rsa_key
```

If any 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:

```
 # chmod 0640 /path/to/file/ssh_host*key
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.203 OL07-00-040430 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that the SSH daemon does not permit Generic Security Service Application Program Interface (GSSAPI) authentication unless needed.

```
GROUP ID: V-221860
RULE ID: SV-221860r958796
```

Rationale:

GSSAPI authentication is used to provide additional authentication mechanisms to applications. Allowing GSSAPI authentication through SSH exposes the system's GSSAPI to remote hosts, increasing the attack surface of the system. GSSAPI authentication must be disabled unless needed.

Audit:

Verify the SSH daemon does not permit GSSAPI authentication unless approved.

Check that the SSH daemon does not permit GSSAPI authentication with the following command:

```
# grep -i gssapiauth /etc/ssh/sshd_config
GSSAPIAuthentication no
```

If the "GSSAPIAuthentication" keyword is missing, is set to "yes" and is not documented with the Information System Security Officer (ISSO), or the returned line is commented out, this is a finding.

Remediation:

Uncomment the "GSSAPIAuthentication" keyword in "/etc/ssh/sshd_config" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor) and set the value to "no":

```
GSSAPIAuthentication no
```

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

If GSSAPI authentication is required, it must be documented, to include the location of the configuration file, with the ISSO.

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)

1.204 OL07-00-040440 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that the SSH daemon does not permit Kerberos authentication unless needed.

```
GROUP ID: V-221861
RULE ID: SV-221861r958796
```

Rationale:

Kerberos authentication for SSH is often implemented using Generic Security Service Application Program Interface (GSSAPI). If Kerberos is enabled through SSH, the SSH daemon provides a means of access to the system's Kerberos implementation. Vulnerabilities in the system's Kerberos implementation may then be subject to exploitation. To reduce the attack surface of the system, the Kerberos authentication mechanism within SSH must be disabled for systems not using this capability.

Audit:

Verify the SSH daemon does not permit Kerberos to authenticate passwords unless approved.

Check that the SSH daemon does not permit Kerberos to authenticate passwords with the following command:

```
# grep -i kerberosauth /etc/ssh/sshd_config
KerberosAuthentication no
```

If the "KerberosAuthentication" keyword is missing, or is set to "yes" and is not documented with the Information System Security Officer (ISSO), or the returned line is commented out, this is a finding.

Remediation:

Uncomment the "KerberosAuthentication" keyword in "/etc/ssh/sshd_config" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor) and set the value to "no":

```
KerberosAuthentication no
```

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

If Kerberos authentication is required, it must be documented, to include the location of the configuration file, with the ISSO.

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)

1.205 OL07-00-040450 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that the SSH daemon performs strict mode checking of home directory configuration files.

```
GROUP ID: V-221862
RULE ID: SV-221862r991589
```

Rationale:

If other users have access to modify user-specific SSH configuration files, they may be able to log on to the system as another user.

Audit:

Verify the SSH daemon performs strict mode checking of home directory configuration files.

The location of the "sshd_config" file may vary if a different daemon is in use.

Inspect the "sshd_config" file with the following command:

```
# grep -i strictmodes /etc/ssh/sshd_config

StrictModes yes
```

If "StrictModes" is set to "no", is missing, or the returned line is commented out, this is a finding.

Remediation:

Uncomment the "StrictModes" keyword in "/etc/ssh/sshd_config" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor) and set the value to "yes":

```
StrictModes yes
```

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

1.206 OL07-00-040460 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that the SSH daemon uses privilege separation.

```
GROUP ID: V-221863
RULE ID: SV-221863r991589
```

Rationale:

SSH daemon privilege separation causes the SSH process to drop root privileges when not needed, which would decrease the impact of software vulnerabilities in the unprivileged section.

Audit:

Verify the SSH daemon performs privilege separation.

Check that the SSH daemon performs privilege separation with the following command:

```
# grep -i usepriv /etc/ssh/sshd_config

UsePrivilegeSeparation sandbox
```

If the "UsePrivilegeSeparation" keyword is set to "no", is missing, or the returned line is commented out, this is a finding.

Remediation:

Uncomment the "UsePrivilegeSeparation" keyword in "/etc/ssh/sshd_config" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor) and set the value to "sandbox" or "yes":

```
UsePrivilegeSeparation sandbox
```

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

1.207 OL07-00-040470 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that the SSH daemon does not allow compression or only allows compression after successful authentication.

```
GROUP ID: V-221864
RULE ID: SV-221864r991589
```

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:

Note: For Oracle Linux 7.4 and above, this requirement is not applicable.

Verify the SSH daemon performs compression after a user successfully authenticates.

Check that the SSH daemon performs compression after a user successfully authenticates with the following command:

```
 # grep -i compression /etc/ssh/sshd_config
 Compression delayed
```

If the "Compression" keyword is set to "yes", is missing, or the returned line is commented out, this is a finding.

Remediation:

Uncomment the "Compression" keyword in "/etc/ssh/sshd_config" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor) on the system and set the value to "delayed" or "no":

```
 Compression no
```

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

1.208 OL07-00-040500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must, for networked systems, synchronize clocks with a server that is synchronized to one of the redundant United States Naval Observatory (USNO) time servers, a time server designated for the appropriate DoD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).

```
GROUP ID: V-221866
RULE ID: SV-221866r1038944
```

Rationale:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside the configured acceptable allowance (drift) may be inaccurate.

Synchronizing internal information system clocks provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

Organizations should consider endpoints that may not have regular access to the authoritative time server (e.g., mobile, teleworking, and tactical endpoints).

Satisfies: SRG-OS-000355-GPOS-00143, SRG-OS-000356-GPOS-00144

Audit:

Check to see if NTP is running in continuous mode.

```
# ps -ef | grep ntp
```

If NTP is not running, check to see if "chronyd" is running in continuous mode:

```
# ps -ef | grep chronyd
```

If NTP or "chronyd" is not running, this is a finding.

If the NTP process is found, then check the "ntp.conf" file for the "maxpoll" option setting:

```
# grep maxpoll /etc/ntp.conf
server 0.rhel.pool.ntp.org iburst maxpoll 16
```

If the "maxpoll" option is set to a number greater than 16 or the line is commented out, this is a finding.

If the file does not exist, check the "/etc/cron.daily" subdirectory for a crontab file controlling the execution of the "ntpd -q" command.

```
# grep -i "ntpd -q" /etc/cron.daily/*
# ls -al /etc/cron.* | grep ntp
ntp
```

If a crontab file does not exist in the "/etc/cron.daily" that executes the "ntpd -q" command, this is a finding.

If the "chronyd" process is found, then check the "chrony.conf" file for the "maxpoll" option setting:

```
# grep maxpoll /etc/chrony.conf

server 0.rhel.pool.ntp.org iburst maxpoll 16
```

If the option is not set or the line is commented out, this is a finding.

Remediation:

Edit the "/etc/ntp.conf" or "/etc/chrony.conf" file and add or update an entry to define "maxpoll" to "16" as follows:

```
server 0.rhel.pool.ntp.org iburst maxpoll 16
```

If NTP was running and "maxpoll" was updated, the NTP service must be restarted:

```
# systemctl restart ntpd
```

If NTP was not running, it must be started:

```
# systemctl start ntpd
```

If "chronyd" was running and "maxpoll" was updated, the service must be restarted:

```
# systemctl restart chronyd.service
```

If "chronyd" was not running, it must be started:

```
# systemctl start chronyd.service
```

Additional Information:

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-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-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)

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)

1.209 OL07-00-040510 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must protect against or limit the effects of Denial of Service (DoS) attacks by validating the operating system is implementing rate-limiting measures on impacted network interfaces.

```
GROUP ID: V-221867
RULE ID: SV-221867r958902
```

Rationale:

DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of the operating system to mitigate the impact of DoS attacks that have occurred or are ongoing on system availability. For each system, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exists to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or establishing memory partitions). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

Audit:

Verify the operating system protects against or limits the effects of DoS attacks by ensuring the operating system is implementing rate-limiting measures on impacted network interfaces.

```
# grep -r net.ipv4.tcp_invalid_ratelimit /run/sysctl.d/* /etc/sysctl.d/*
/usr/local/lib/sysctl.d/* /usr/lib/sysctl.d/* /lib/sysctl.d/*
/etc/sysctl.conf 2> /dev/null
/etc/sysctl.conf:net.ipv4.tcp_invalid_ratelimit = 500
```

If "net.ipv4.tcp_invalid_ratelimit" is not configured in the /etc/sysctl.conf file or in any of the other sysctl.d directories, is commented out this is a finding.

Check that the operating system implements the value of the "tcp_invalid_ratelimit" variable with the following command:

```
# /sbin/sysctl -a | grep net.ipv4.tcp_invalid_ratelimit
net.ipv4.tcp_invalid_ratelimit = 500
```

If "net.ipv4.tcp_invalid_ratelimit" has a value of "0", this is a finding.

If "net.ipv4.tcp_invalid_ratelimit" has a value greater than "1000" and is not documented with the Information System Security Officer (ISSO), this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Set the system to implement rate-limiting measures by adding the following line to "/etc/sysctl.conf" or a configuration file in the /etc/sysctl.d/ directory (or modify the line to have the required value):

```
net.ipv4.tcp_invalid_ratelimit = 500
```

Issue the following command to make the changes take effect:

```
# sysctl --system
```

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

1.210 OL07-00-040520 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must enable an application firewall, if available.

```
GROUP ID: V-221868
RULE ID: SV-221868r991589
```

Rationale:

Firewalls protect computers from network attacks by blocking or limiting access to open network ports. Application firewalls limit which applications are allowed to communicate over the network.

Satisfies: SRG-OS-000480-GPOS-00227, SRG-OS-000480-GPOS-00231, SRG-OS-000480-GPOS-00232

Audit:

Verify the operating system enabled an application firewall.

Check to see if "firewalld" is installed with the following command:

```
# yum list installed firewalld
firewalld-0.3.9-11.el7.noarch.rpm
```

If the "firewalld" package is not installed, ask the System Administrator if another firewall application (such as iptables) is installed.

If an application firewall is not installed, this is a finding.

Check to see if the firewall is loaded and active with the following command:

```
# systemctl status firewalld
firewalld.service - firewalld - dynamic firewall daemon

Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled)
Active: active (running) since Tue 2014-06-17 11:14:49 CEST; 5 days ago
```

If "firewalld" does not show a status of "loaded" and "active", this is a finding.

Check the state of the firewall:

```
# firewall-cmd --state
running
```

If "firewalld" does not show a state of "running", this is a finding.

Remediation:

Ensure the operating system's application firewall is enabled.

Install the "firewalld" package, if it is not on the system, with the following command:

```
# yum install firewalld
```

Start the firewall via "systemctl" with the following command:

```
# systemctl start firewalld
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.211 OL07-00-040530 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Oracle Linux operating system must display the date and time of the last successful account logon upon logon.

```
GROUP ID: V-221869
RULE ID: SV-221869r991589
```

Rationale:

Providing users with feedback on when account accesses last occurred facilitates user recognition and reporting of unauthorized account use.

Audit:

Verify users are provided with feedback on when account accesses last occurred.

Check that "pam_lastlog" is used and not silent with the following command:

```
# grep pam_lastlog /etc/pam.d/postlogin
session required pam_lastlog.so showfailed
```

If "pam_lastlog" is missing from "/etc/pam.d/postlogin" file, or the silent option is present, this is a finding.

Remediation:

Configure the operating system to provide users with feedback on when account accesses last occurred by setting the required configuration options in "/etc/pam.d/postlogin".

Add the following line to the top of "/etc/pam.d/postlogin":

```
session required pam_lastlog.so showfailed
```

Additional Information:

CCI-000052 Notify the user, upon successful logon (access) to the system, of the date and time of the last logon (access).

- NIST SP 800-53::AC-9
- NIST SP 800-53A::AC-9.1
- NIST SP 800-53 Revision 4::AC-9
- NIST SP 800-53 Revision 5::AC-9

1.212 OL07-00-040540 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must not contain .shosts files.

```
GROUP ID: V-221870
RULE ID: SV-221870r991589
```

Rationale:

The .shosts files are used to configure host-based authentication for individual users or the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

Audit:

Verify there are no ".shosts" files on the system.

Check the system for the existence of these files with the following command:

```
# find / -name '*.shosts'
```

If any ".shosts" files are found on the system, this is a finding.

Remediation:

Remove any found ".shosts" files from the system.

```
# rm /[path]/[to]/[file]/.shosts
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.213 OL07-00-040550 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must not contain shosts.equiv files.

```
GROUP ID: V-221871
RULE ID: SV-221871r991589
```

Rationale:

The shosts.equiv files are used to configure host-based authentication for the system via SSH. Host-based authentication is not sufficient for preventing unauthorized access to the system, as it does not require interactive identification and authentication of a connection request, or for the use of two-factor authentication.

Audit:

Verify there are no "shosts.equiv" files on the system.

Check the system for the existence of these files with the following command:

```
# find / -name shosts.equiv
```

If any "shosts.equiv" files are found on the system, this is a finding.

Remediation:

Remove any found "shosts.equiv" files from the system.

```
# rm /[path]/[to]/[file]/shosts.equiv
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.214 OL07-00-040600 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

For Oracle Linux operating systems using DNS resolution, at least two name servers must be configured.

```
GROUP ID: V-221872
RULE ID: SV-221872r991589
```

Rationale:

To provide availability for name resolution services, multiple redundant name servers are mandated. A failure in name resolution could lead to the failure of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.

Audit:

Determine whether the system is using local or DNS name resolution with the following command:

```
# grep hosts /etc/nsswitch.conf
hosts: files dns
```

If the DNS entry is missing from the host's line in the "/etc/nsswitch.conf" file, the "/etc/resolv.conf" file must be empty.

Verify the "/etc/resolv.conf" file is empty with the following command:

```
# ls -al /etc/resolv.conf
-rw-r--r-- 1 root root 0 Aug 19 08:31 resolv.conf
```

If local host authentication is being used and the "/etc/resolv.conf" file is not empty, this is a finding.

If the DNS entry is found on the host's line of the "/etc/nsswitch.conf" file, verify the operating system is configured to use two or more name servers for DNS resolution.

Determine the name servers used by the system with the following command:

```
# grep nameserver /etc/resolv.conf
nameserver 192.168.1.2
nameserver 192.168.1.3
```

If less than two lines are returned that are not commented out, this is a finding.

Verify the "/etc/resolv.conf" file is immutable with the following command:

```
# sudo lsattr /etc/resolv.conf

----i----------- /etc/resolv.conf
```

If the file is mutable and has not been documented with the Information System Security Officer (ISSO), this is a finding.

Remediation:

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

Edit the "/etc/resolv.conf" file to uncomment or add the two or more "nameserver" option lines with the IP address of local authoritative name servers. If local host resolution is being performed, the "/etc/resolv.conf" file must be empty. An empty "/etc/resolv.conf" file can be created as follows:

```
# echo -n > /etc/resolv.conf
```

And then make the file immutable with the following command:

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

If the "/etc/resolv.conf" file must be mutable, the required configuration must be documented with the Information System Security Officer (ISSO) and the file must be verified by the system file integrity tool.

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.215 OL07-00-040610 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must not forward Internet Protocol version 4 (IPv4) source-routed packets.

```
GROUP ID: V-221873
RULE ID: SV-221873r991589
```

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 IPv4 forwarding is enabled and the system is functioning as a router.

Audit:

Verify the system does not accept IPv4 source-routed packets.

```
 # grep -r net.ipv4.conf.all.accept_source_route /run/sysctl.d/*
/etc/sysctl.d/* /usr/local/lib/sysctl.d/* /usr/lib/sysctl.d/* /lib/sysctl.d/*
/etc/sysctl.conf 2> /dev/null
 net.ipv4.conf.all.accept_source_route = 0
```

If "net.ipv4.conf.all.accept_source_route" is not configured in the /etc/sysctl.conf file or in any of the other sysctl.d directories, is commented out, or does not have a value of "0", this is a finding.

Check that the operating system implements the accept source route variable with the following command:

```
 # /sbin/sysctl -a | grep 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", this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Set the system to the required kernel parameter by adding the following line to "/etc/sysctl.conf" or a configuration file in the /etc/sysctl.d/ directory (or modify the line to have the required value):

```
net.ipv4.conf.all.accept_source_route = 0
```

Issue the following command to make the changes take effect:

```
# sysctl -system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.216 OL07-00-040611 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must use a reverse-path filter for IPv4 network traffic when possible on all interfaces.

```
GROUP ID: V-221874
RULE ID: SV-221874r991589
```

Rationale:

Enabling reverse path filtering drops packets with invalid source addresses received on the interface. It should not be used on systems that are routers for complicated networks, but is helpful for end hosts and routers serving small networks.

Audit:

Verify the system uses a reverse-path filter for IPv4:

```
 # grep -r net.ipv4.conf.all.rp_filter /run/sysctl.d/* /etc/sysctl.d/*
/usr/local/lib/sysctl.d/* /usr/lib/sysctl.d/* /lib/sysctl.d/*
/etc/sysctl.conf 2> /dev/null
 net.ipv4.conf.all.rp_filter = 1
```

If "net.ipv4.conf.all.rp_filter" is not configured in the /etc/sysctl.conf file or in any of the other sysctl.d directories, is commented out, or does not have a value of "1", this is a finding.

Check that the operating system implements the accept source route variable with the following command:

```
 # /sbin/sysctl -a | grep net.ipv4.conf.all.rp_filter
 net.ipv4.conf.all.rp_filter = 1
```

If the returned line does not have a value of "1", this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Set the system to the required kernel parameter by adding the following line to "/etc/sysctl.conf" or a configuration file in the /etc/sysctl.d/ directory (or modify the line to have the required value):

```
net.ipv4.conf.all.rp_filter = 1
```

Issue the following command to make the changes take effect:

```
# sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.217 OL07-00-040612 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must use a reverse-path filter for IPv4 network traffic when possible by default.

```
GROUP ID: V-221875
RULE ID: SV-221875r991589
```

Rationale:

Enabling reverse path filtering drops packets with invalid source addresses received on the interface. It should not be used on systems which are routers for complicated networks, but is helpful for end hosts and routers serving small networks.

Audit:

Verify the system uses a reverse-path filter for IPv4:

```
 # grep -r net.ipv4.conf.default.rp_filter /run/sysctl.d/* /etc/sysctl.d/*
/usr/local/lib/sysctl.d/* /usr/lib/sysctl.d/* /lib/sysctl.d/*
/etc/sysctl.conf 2> /dev/null
 net.ipv4.conf.default.rp_filter = 1
```

If "net.ipv4.conf.default.rp_filter" is not configured in the /etc/sysctl.conf file or in any of the other sysctl.d directories, is commented out, or does not have a value of "1", this is a finding.

Check that the operating system implements the accept source route variable with the following command:

```
 # /sbin/sysctl -a | grep net.ipv4.conf.default.rp_filter
 net.ipv4.conf.default.rp_filter = 1
```

If the returned line does not have a value of "1", this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Set the system to the required kernel parameter by adding the following line to "/etc/sysctl.conf" or a configuration file in the /etc/sysctl.d/ directory (or modify the line to have the required value):

```
net.ipv4.conf.default.rp_filter = 1
```

Issue the following command to make the changes take effect:

```
# sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.218 OL07-00-040620 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must not forward Internet Protocol version 4 (IPv4) source-routed packets by default.

```
GROUP ID: V-221876
RULE ID: SV-221876r991589
```

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 IPv4 forwarding is enabled and the system is functioning as a router.

Audit:

Verify the system does not accept IPv4 source-routed packets by default.

```
 # grep -r net.ipv4.conf.default.accept_source_route /run/sysctl.d/*
/etc/sysctl.d/* /usr/local/lib/sysctl.d/* /usr/lib/sysctl.d/* /lib/sysctl.d/*
/etc/sysctl.conf 2> /dev/null
 net.ipv4.conf.default.accept_source_route = 0
```

If "net.ipv4.conf.default.accept_source_route" is not configured in the /etc/sysctl.conf file or in any of the other sysctl.d directories, is commented out, or does not have a value of "0", this is a finding.

Check that the operating system implements the accept source route variable with the following command:

```
 # /sbin/sysctl -a | grep 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", this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Set the system to the required kernel parameter by adding the following line to "/etc/sysctl.conf" or a configuration file in the /etc/sysctl.d/ directory (or modify the line to have the required value):

```
net.ipv4.conf.default.accept_source_route = 0
```

Issue the following command to make the changes take effect:

```
# sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.219 OL07-00-040630 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must not respond to Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) echoes sent to a broadcast address.

```
GROUP ID: V-221877
RULE ID: SV-221877r991589
```

Rationale:

Responding to broadcast (ICMP) echoes facilitates network mapping and provides a vector for amplification attacks.

Audit:

Verify the system does not respond to IPv4 ICMP echoes sent to a broadcast address.

```
 # grep -r net.ipv4.icmp_echo_ignore_broadcasts /run/sysctl.d/*
/etc/sysctl.d/* /usr/local/lib/sysctl.d/* /usr/lib/sysctl.d/* /lib/sysctl.d/*
/etc/sysctl.conf 2> /dev/null
```

If "net.ipv4.icmp_echo_ignore_broadcasts" is not configured in the /etc/sysctl.conf file or in any of the other sysctl.d directories, is commented out, or does not have a value of "1", this is a finding.

Check that the operating system implements the "icmp_echo_ignore_broadcasts" variable with the following command:

```
 # /sbin/sysctl -a | grep net.ipv4.icmp_echo_ignore_broadcasts
 net.ipv4.icmp_echo_ignore_broadcasts = 1
```

If the returned line does not have a value of "1", this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Set the system to the required kernel parameter by adding the following line to "/etc/sysctl.conf" or a configuration file in the /etc/sysctl.d/ directory (or modify the line to have the required value):

```
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

Issue the following command to make the changes take effect:

```
# sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.220 OL07-00-040640 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must prevent Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages from being accepted.

```
GROUP ID: V-221878
RULE ID: SV-221878r991589
```

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 the system will not accept IPv4 ICMP redirect messages.

```
 # grep -r net.ipv4.conf.default.accept_redirects /run/sysctl.d/*
/etc/sysctl.d/* /usr/local/lib/sysctl.d/* /usr/lib/sysctl.d/* /lib/sysctl.d/*
/etc/sysctl.conf 2> /dev/null
```

If "net.ipv4.conf.default.accept_redirects" is not configured in the /etc/sysctl.conf file or in any of the other sysctl.d directories, is commented out, or does not have a value of "0", this is a finding.

Check that the operating system implements the value of the "accept_redirects" variables with the following command:

```
 # /sbin/sysctl -a | grep net.ipv4.conf.default.accept_redirects
 net.ipv4.conf.default.accept_redirects = 0
```

If the returned line does not have a value of "0", this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Set the system to not accept IPv4 ICMP redirect messages by adding the following line to "/etc/sysctl.conf" or a configuration file in the /etc/sysctl.d/ directory (or modify the line to have the required value):

```
net.ipv4.conf.default.accept_redirects = 0
```

Issue the following command to make the changes take effect:

```
# sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.221 OL07-00-040641 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must ignore Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages.

```
GROUP ID: V-221879
RULE ID: SV-221879r991589
```

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 the system ignores IPv4 ICMP redirect messages.

```
 # grep -r net.ipv4.conf.all.accept_redirects /run/sysctl.d/* /etc/sysctl.d/*
/usr/local/lib/sysctl.d/* /usr/lib/sysctl.d/* /lib/sysctl.d/*
/etc/sysctl.conf 2> /dev/null
```

If "net.ipv4.conf.all.accept_redirects" is not configured in the /etc/sysctl.conf file or in any of the other sysctl.d directories, is commented out, or does not have a value of "0", this is a finding.

Check that the operating system implements the "accept_redirects" variables with the following command:

```
 # /sbin/sysctl -a | grep net.ipv4.conf.all.accept_redirects
 net.ipv4.conf.all.accept_redirects = 0
```

If the returned line does not have a value of "0", this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Set the system to ignore IPv4 ICMP redirect messages by adding the following line to "/etc/sysctl.conf" or a configuration file in the /etc/sysctl.d/ directory (or modify the line to have the required value):

```
net.ipv4.conf.all.accept_redirects = 0
```

Issue the following command to make the changes take effect:

```
# sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.222 OL07-00-040650 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must not allow interfaces to perform Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects by default.

```
GROUP ID: V-221880
RULE ID: SV-221880r991589
```

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.

Audit:

Verify the system does not allow interfaces to perform IPv4 ICMP redirects by default.

```
 # grep -r net.ipv4.conf.default.send_redirects /run/sysctl.d/*
/etc/sysctl.d/* /usr/local/lib/sysctl.d/* /usr/lib/sysctl.d/* /lib/sysctl.d/*
/etc/sysctl.conf 2> /dev/null
```

If "net.ipv4.conf.default.send_redirects" is not configured in the "/etc/sysctl.conf" file or in any of the other sysctl.d directories, is commented out or does not have a value of "0", this is a finding.

Check that the operating system implements the "default send_redirects" variables with the following command:

```
 # /sbin/sysctl -a | grep net.ipv4.conf.default.send_redirects
 net.ipv4.conf.default.send_redirects = 0
```

If the returned line does not have a value of "0", this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure the system not to allow interfaces to perform IPv4 ICMP redirects by default.

Set the system to the required kernel parameter by adding the following line to "/etc/sysctl.conf" or a configuration file in the /etc/sysctl.d/ directory (or modify the line to have the required value):

```
net.ipv4.conf.default.send_redirects = 0
```

Issue the following command to make the changes take effect:

```
# sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.223 OL07-00-040660 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must not send Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects.

```
GROUP ID: V-221881
RULE ID: SV-221881r991589
```

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.

Audit:

Verify the system does not send IPv4 ICMP redirect messages.

```
 # grep -r net.ipv4.conf.all.send_redirects /run/sysctl.d/* /etc/sysctl.d/*
/usr/local/lib/sysctl.d/* /usr/lib/sysctl.d/* /lib/sysctl.d/*
/etc/sysctl.conf 2> /dev/null
```

If "net.ipv4.conf.all.send_redirects" is not configured in the /etc/sysctl.conf file or in any of the other sysctl.d directories, is commented out or does not have a value of "0", this is a finding.

Check that the operating system implements the "all send_redirects" variables with the following command:

```
 # /sbin/sysctl -a | grep net.ipv4.conf.all.send_redirects
 net.ipv4.conf.all.send_redirects = 0
```

If the returned line does not have a value of "0", this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Configure the system not to allow interfaces to perform IPv4 ICMP redirects.

Set the system to the required kernel parameter by adding the following line to "/etc/sysctl.conf" or a configuration file in the /etc/sysctl.d/ directory (or modify the line to have the required value):

```
net.ipv4.conf.all.send_redirects = 0
```

Issue the following command to make the changes take effect:

```
# sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.224 OL07-00-040670 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Network interfaces configured on The Oracle Linux operating system must not be in promiscuous mode.

```
GROUP ID: V-221882
RULE ID: SV-221882r991589
```

Rationale:

Network interfaces in promiscuous mode allow for the capture of all network traffic visible to the system. If unauthorized individuals can access these applications, it may allow them to collect information such as logon IDs, passwords, and key exchanges between systems.

If the system is being used to perform a network troubleshooting function, the use of these tools must be documented with the Information System Security Officer (ISSO) and restricted to authorized personnel only.

Audit:

Verify network interfaces are not in promiscuous mode unless approved by the ISSO and documented.

Check for the status with the following command:

```
# ip link | grep -i promisc
```

If network interfaces are found on the system in promiscuous mode and their use has not been approved by the ISSO and documented, this is a finding.

Remediation:

Configure network interfaces to turn off promiscuous mode unless approved by the ISSO and documented.

Set the promiscuous mode of an interface to off with the following command:

```
#ip link set dev <devicename> multicast off promisc off
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.225 OL07-00-040680 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured to prevent unrestricted mail relaying.

```
GROUP ID: V-221883
RULE ID: SV-221883r991589
```

Rationale:

If unrestricted mail relaying is permitted, unauthorized senders could use this host as a mail relay for the purpose of sending spam or other unauthorized activity.

Audit:

Verify the system is configured to prevent unrestricted mail relaying.

Determine if "postfix" is installed with the following commands:

```
# yum list installed postfix
postfix-2.6.6-6.el7.x86_64.rpm
```

If postfix is not installed, this is Not Applicable.

If postfix is installed, determine if it is configured to reject connections from unknown or untrusted networks with the following command:

```
# postconf -n smtpd_client_restrictions
smtpd_client_restrictions = permit_mynetworks, reject
```

If the "smtpd_client_restrictions" parameter contains any entries other than "permit_mynetworks" and "reject", this is a finding.

Remediation:

If "postfix" is installed, modify the "/etc/postfix/main.cf" file to restrict client connections to the local network with the following command:

```
# postconf -e 'smtpd_client_restrictions = permit_mynetworks,reject'
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.226 OL07-00-040690 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must not have a File Transfer Protocol (FTP) server package installed unless needed.

```
GROUP ID: V-221884
RULE ID: SV-221884r991589
```

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.

Audit:

Verify an FTP server has not been installed on the system.

Check to see if an FTP server has been installed with the following commands:

```
# yum list installed vsftpd

vsftpd-3.0.2.el7.x86_64.rpm
```

If "vsftpd" is installed and is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Document the "vsftpd" package with the ISSO as an operational requirement or remove it from the system with the following command:

```
# yum remove vsftpd
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.227 OL07-00-040700 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Oracle Linux operating system must not have the Trivial File Transfer Protocol (TFTP) server package installed if not required for operational support.

```
GROUP ID: V-221885
RULE ID: SV-221885r991589
```

Rationale:

If TFTP is required for operational support (such as the transmission of router configurations) its use must be documented with the Information System Security Officer (ISSO), restricted to only authorized personnel, and have access control rules established.

Audit:

Verify a TFTP server has not been installed on the system.

Check to see if a TFTP server has been installed with the following command:

```
# yum list installed tftp-server
tftp-server-0.49-9.el7.x86_64.rpm
```

If TFTP is installed and the requirement for TFTP is not documented with the ISSO, this is a finding.

Remediation:

Remove the TFTP package from the system with the following command:

```
# yum remove tftp-server
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.228 OL07-00-040710 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that remote X connections are disabled, unless to fulfill documented and validated mission requirements.

```
GROUP ID: V-221886
RULE ID: SV-221886r991589
```

Rationale:

The security risk of using X11 forwarding is that the client's X11 display server may be exposed to attack when the SSH client requests forwarding. A system administrator may have a stance in which they want to protect clients that may expose themselves to attack by unwittingly requesting X11 forwarding, which can warrant a "no" setting. X11 forwarding should be enabled with caution. Users with the ability to bypass file permissions on the remote host (for the user's X11 authorization database) can access the local X11 display through the forwarded connection. An attacker may then be able to perform activities such as keystroke monitoring if the ForwardX11Trusted option is also enabled. If X11 services are not required for the system's intended function, they should be disabled or restricted as appropriate to the system’s needs.

Audit:

Determine if X11Forwarding is disabled with the following command:

```
# grep -i x11forwarding /etc/ssh/sshd_config | grep -v "^#"

X11Forwarding no
```

If the "X11Forwarding" keyword is set to "yes" and is not documented with the Information System Security Officer (ISSO) as an operational requirement or is missing, this is a finding.

Remediation:

Edit the "/etc/ssh/sshd_config" file to uncomment or add the line for the "X11Forwarding" keyword and set its value to "no" (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):

```
X11Forwarding no
```

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

```
# systemctl restart sshd
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.229 OL07-00-040711 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system SSH daemon must prevent remote hosts from connecting to the proxy display.

```
GROUP ID: V-233306
RULE ID: SV-233306r991589
```

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 DIPSLAY environment variable to localhost. This prevents remote hosts from connecting to the proxy display.

Audit:

Verify the SSH daemon prevents remote hosts from connecting to the proxy display.

Check the SSH X11UseLocalhost setting with the following command:

```
# sudo grep -i x11uselocalhost /etc/ssh/sshd_config
X11UseLocalhost yes
```

If the "X11UseLocalhost" keyword is set to "no", is missing, or is commented out, this is a finding.

Remediation:

Configure the SSH daemon to prevent remote hosts from connecting to the proxy display.

Edit the "/etc/ssh/sshd_config" file to uncomment or add the line for the "X11UseLocalhost" keyword and set its value to "yes" (this file may be named differently or be in a different location if using a version of SSH that is provided by a third-party vendor):

```
X11UseLocalhost yes
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.230 OL07-00-040712 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system SSH server must be configured to use only FIPS-validated key exchange algorithms.

```
GROUP ID: V-255899
RULE ID: SV-255899r958408
```

Rationale:

The use of FIPS-validated cryptographic algorithms is enforced by enabling kernel FIPS mode. In the event that kernel FIPS mode is disabled, the use of nonvalidated cryptographic algorithms will be permitted systemwide. The SSH server configuration must manually define only FIPS-validated key exchange algorithms to prevent the use of nonvalidated algorithms.

Audit:

Verify that the SSH server is configured to use only FIPS-validated key exchange algorithms:

```
 $ sudo grep -i kexalgorithms /etc/ssh/sshd_config
 KexAlgorithms ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-
nistp521,diffie-hellman-group-exchange-sha256
```

If "KexAlgorithms" is not configured, is commented out, or does not contain only the algorithms "ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256" in exact order, this is a finding.

Remediation:

Configure the SSH server to use only FIPS-validated key exchange algorithms by adding or modifying the following line in "/etc/ssh/sshd_config":

```
 KexAlgorithms ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-
nistp521,diffie-hellman-group-exchange-sha256
```

Restart the "sshd" service for changes to take effect:

```
 $ sudo systemctl restart sshd
```

Additional Information:

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

1.231 OL07-00-040720 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that if the Trivial File Transfer Protocol (TFTP) server is required, the TFTP daemon is configured to operate in secure mode.

```
GROUP ID: V-221887
RULE ID: SV-221887r991589
```

Rationale:

Restricting TFTP to a specific directory prevents remote users from copying, transferring, or overwriting system files.

Audit:

Verify the TFTP daemon is configured to operate in secure mode.

Check to see if a TFTP server has been installed with the following commands:

```
# yum list installed tftp-server
tftp-server.x86_64 x.x-x.el7
```

If a TFTP server is not installed, this is Not Applicable.

If a TFTP server is installed, check for the server arguments with the following command:

```
# grep server_args /etc/xinetd.d/tftp
server_args = -s /var/lib/tftpboot
```

If the "server_args" line does not have a "-s" option and a subdirectory is not assigned, this is a finding.

Remediation:

Configure the TFTP daemon to operate in secure mode by adding the following line to "/etc/xinetd.d/tftp" (or modify the line to have the required value):

```
server_args = -s /var/lib/tftpboot
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.232 OL07-00-040730 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must not have a graphical display manager installed unless approved.

```
GROUP ID: V-221888
RULE ID: SV-221888r991589
```

Rationale:

Internet services not required for system or application processes must not be active to decrease the attack surface of the system. Graphical display managers have a long history of security vulnerabilities and must not be used unless approved and documented.

Audit:

Verify the system 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.

Verify that a graphical user interface is not installed:

```
$ rpm -qa | grep xorg | grep server
```

Ask the System Administrator if use of a graphical user interface is an operational requirement.

If the use of a graphical user interface on the system is not documented with the ISSO, this is a finding.

Remediation:

Document the requirement for a graphical user interface with the ISSO or reinstall the operating system without the graphical user interface. If reinstallation is not feasible, then continue with the following procedure:

Open an SSH session and enter the following commands:

```
$ sudo systemctl set-default multi-user.target
$ sudo yum remove xorg-x11-server-Xorg xorg-x11-server-common xorg-x11-
server-utils
```

A reboot is required for the changes to take effect.

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.233 OL07-00-040740 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must not be performing packet forwarding unless the system is a router.

```
GROUP ID: V-221889
RULE ID: SV-221889r991589
```

Rationale:

Routing protocol daemons are typically used on routers to exchange network topology information with other routers. If this software is used when not required, system network information may be unnecessarily transmitted across the network.

Audit:

Verify the system is not performing packet forwarding, unless the system is a router.

```
 # grep -r net.ipv4.ip_forward /run/sysctl.d/* /etc/sysctl.d/*
/usr/local/lib/sysctl.d/* /usr/lib/sysctl.d/* /lib/sysctl.d/*
/etc/sysctl.conf 2> /dev/null
 net.ipv4.ip_forward = 0
```

If "net.ipv4.ip_forward" is not configured in the /etc/sysctl.conf file or in any of the other sysctl.d directories, is commented out, or does not have a value of "0", this is a finding.

Check that the operating system does not implement IP forwarding using the following command:

```
 # /sbin/sysctl -a | grep net.ipv4.ip_forward
 net.ipv4.ip_forward = 0
```

If IP forwarding value is "1" and the system is hosting any application, database, or web servers, this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Set the system to the required kernel parameter by adding the following line to "/etc/sysctl.conf" or a configuration file in the /etc/sysctl.d/ directory (or modify the line to have the required value):

```
net.ipv4.ip_forward = 0
```

Issue the following command to make the changes take effect:

```
# sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.234 OL07-00-040750 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that the Network File System (NFS) is configured to use RPCSEC_GSS.

```
GROUP ID: V-221890
RULE ID: SV-221890r991589
```

Rationale:

When an NFS server is configured to use RPCSEC_SYS, a selected userid and groupid are used to handle requests from the remote user. The userid and groupid could mistakenly or maliciously be set incorrectly. The RPCSEC_GSS method of authentication uses certificates on the server and client systems to more securely authenticate the remote mount request.

Audit:

Verify "AUTH_GSS" is being used to authenticate NFS mounts.

To check if the system is importing an NFS file system, look for any entries in the "/etc/fstab" file that have a file system type of "nfs" with the following command:

```
# cat /etc/fstab | grep nfs
192.168.21.5:/mnt/export /data1 nfs4 rw,sync ,soft,sec=krb5:krb5i:krb5p
```

If the system is mounting file systems via NFS and has the sec option without the "krb5:krb5i:krb5p" settings, the "sec" option has the "sys" setting, or the "sec" option is missing, this is a finding.

Remediation:

Update the "/etc/fstab" file so the option "sec" is defined for each NFS mounted file system and the "sec" option does not have the "sys" setting.

Ensure the "sec" option is defined as "krb5:krb5i:krb5p".

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.235 OL07-00-040800 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

SNMP community strings on the Oracle Linux operating system must be changed from the default.

```
GROUP ID: V-221891
RULE ID: SV-221891r991589
```

Rationale:

Whether active or not, default Simple Network Management Protocol (SNMP) community strings must be changed to maintain security. If the service is running with the default authenticators, anyone can gather data about the system and the network and use the information to potentially compromise the integrity of the system or network(s). It is highly recommended that SNMP version 3 user authentication and message encryption be used in place of the version 2 community strings.

Audit:

Verify that a system using SNMP is not using default community strings.

Check to see if the "/etc/snmp/snmpd.conf" file exists with the following command:

```
# ls -al /etc/snmp/snmpd.conf
-rw------- 1 root root 52640 Mar 12 11:08 snmpd.conf
```

If the file does not exist, this is Not Applicable.

If the file does exist, check for the default community strings with the following commands:

```
# grep public /etc/snmp/snmpd.conf
# grep private /etc/snmp/snmpd.conf
```

If either of these commands returns any output, this is a finding.

Remediation:

If the "/etc/snmp/snmpd.conf" file exists, modify any lines that contain a community string value of "public" or "private" to another string value.

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.236 OL07-00-040810 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system access control program must be configured to grant or deny system access to specific hosts and services.

```
GROUP ID: V-221892
RULE ID: SV-221892r991589
```

Rationale:

If the systems access control program is not configured with appropriate rules for allowing and denying access to system network resources, services may be accessible to unauthorized hosts.

Audit:

If the "firewalld" package is not installed, ask the System Administrator (SA) if another firewall application (such as iptables) is installed. If an application firewall is not installed, this is a finding.

Verify the system's access control program is configured to grant or deny system access to specific hosts.

Check to see if "firewalld" is active with the following command:

```
# systemctl status firewalld
firewalld.service - firewalld - dynamic firewall daemon
Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled)
Active: active (running) since Sun 2014-04-20 14:06:46 BST; 30s ago
```

If "firewalld" is active, check to see if it is configured to grant or deny access to specific hosts or services with the following commands:

```
# firewall-cmd --get-default-zone
public
# firewall-cmd --list-all --zone=public
public (active)
target: default
icmp-block-inversion: no
interfaces: eth0
sources:
services: mdns ssh
ports:
protocols:
masquerade: no
forward-ports:
icmp-blocks:
```

If "firewalld" is not active, determine whether "tcpwrappers" is being used by checking whether the "hosts.allow" and "hosts.deny" files are empty with the following commands:

```
# ls -al /etc/hosts.allow
rw-r----- 1 root root 9 Aug 2 23:13 /etc/hosts.allow
# ls -al /etc/hosts.deny
-rw-r----- 1 root root 9 Apr 9 2007 /etc/hosts.deny
```

If "firewalld" and "tcpwrappers" are not installed, configured, and active, ask the SA if another access control program (such as iptables) is installed and active. Ask the SA to show that the running configuration grants or denies access to specific hosts or services.

If "firewalld" is active and is not configured to grant access to specific hosts or "tcpwrappers" is not configured to grant or deny access to specific hosts, this is a finding.

Remediation:

If "firewalld" is installed and active on the system, configure rules for allowing specific services and hosts.

If "firewalld" is not "active", enable "tcpwrappers" by configuring "/etc/hosts.allow" and "/etc/hosts.deny" to allow or deny access to specific hosts.

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.237 OL07-00-040820 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must not have unauthorized IP tunnels configured.

```
GROUP ID: V-221893
RULE ID: SV-221893r991589
```

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 the system does not have unauthorized IP tunnels configured.

Check to see if "libreswan" is installed with the following command:

```
# yum list installed libreswan
libreswan.x86-64 3.20-5.el7_4
```

If "libreswan" is installed, check to see if the "IPsec" service is active with the following command:

```
# systemctl status ipsec
ipsec.service - Internet Key Exchange (IKE) Protocol Daemon for IPsec
Loaded: loaded (/usr/lib/systemd/system/ipsec.service; disabled)
Active: inactive (dead)
```

If the "IPsec" service is active, check to see if any tunnels are configured in "/etc/ipsec.conf" and "/etc/ipsec.d/" with the following commands:

```
# grep -iw conn /etc/ipsec.conf /etc/ipsec.d/*.conf
```

If there are indications that a "conn" parameter is configured for a tunnel, ask the System Administrator if the tunnel is documented with the ISSO.

If "libreswan" is installed, "IPsec" is active, and an undocumented tunnel is active, 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 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.238 OL07-00-040830 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must not forward IPv6 source-routed packets.

```
GROUP ID: V-221894
RULE ID: SV-221894r991589
```

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 IPv6 forwarding is enabled and the system is functioning as a router.

Audit:

If IPv6 is not enabled, the key will not exist, and this is Not Applicable.

Verify the system does not accept IPv6 source-routed packets.

```
 # grep -r net.ipv6.conf.all.accept_source_route /run/sysctl.d/*
/etc/sysctl.d/* /usr/local/lib/sysctl.d/* /usr/lib/sysctl.d/* /lib/sysctl.d/*
/etc/sysctl.conf 2> /dev/null
 net.ipv6.conf.all.accept_source_route = 0
```

If "net.ipv6.conf.all.accept_source_route" is not configured in the /etc/sysctl.conf file or in any of the other sysctl.d directories, is commented out or does not have a value of "0", this is a finding.

Check that the operating system implements the accept source route variable with the following command:

```
 # /sbin/sysctl -a | grep net.ipv6.conf.all.accept_source_route
 net.ipv6.conf.all.accept_source_route = 0
```

If the returned lines do not have a value of "0", this is a finding.

If conflicting results are returned, this is a finding.

Remediation:

Set the system to the required kernel parameter, if IPv6 is enabled, by adding the following line to "/etc/sysctl.conf" or a configuration file in the /etc/sysctl.d/ directory (or modify the line to have the required value):

```
net.ipv6.conf.all.accept_source_route = 0
```

Issue the following command to make the changes take effect:

```
# sysctl --system
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.239 OL07-00-041001 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must have the required packages for multifactor authentication installed.

```
GROUP ID: V-221895
RULE ID: SV-221895r1015191
```

Rationale:

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

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

Audit:

Verify the operating system has the packages required for multifactor authentication installed.

Check for the presence of the packages required to support multifactor authentication with the following commands:

```
# yum list installed pam_pkcs11
pam_pkcs11-0.6.2-14.el7.noarch.rpm
```

If the "pam_pkcs11" packages is not installed, this is a finding.

Remediation:

Configure the operating system to implement multifactor authentication by installing the required packages.

Install the "pam_pkcs11" package with the following command:

```
# yum install pam_pkcs11
```

Additional Information:

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)

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 Accept 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 verify Personal Identity Verification-compliant credentials.

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

1.240 OL07-00-041002 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must implement multifactor authentication for access to privileged accounts via pluggable authentication modules (PAM).

```
GROUP ID: V-221896
RULE ID: SV-221896r1015192
```

Rationale:

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

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

Audit:

Verify the operating system implements multifactor authentication for remote access to privileged accounts via pluggable authentication modules (PAM).

Check the "/etc/sssd/sssd.conf" file for the authentication services that are being used with the following command:

```
# grep services /etc/sssd/sssd.conf /etc/sssd/conf.d/*.conf

services = nss, pam
```

If the "pam" service is not present on all "services" lines, this is a finding.

Remediation:

Configure the operating system to implement multifactor authentication for remote access to privileged accounts via pluggable authentication modules (PAM).

Modify all of the services lines in "/etc/sssd/sssd.conf" or in configuration files found under "/etc/sssd/conf.d" to include pam.

Additional Information:

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)

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 Accept 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 verify Personal Identity Verification-compliant credentials.

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

1.241 OL07-00-041003 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must implement certificate status checking for PKI authentication.

```
GROUP ID: V-221897
RULE ID: SV-221897r1015193
```

Rationale:

Using an authentication device, such as a CAC or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD Common Access Card.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DoD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components where this is specific to the function of the device or has the concept of an organizational user (e.g., VPN, proxy capability). This does not apply to authentication for the purpose of configuring the device itself (management).

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

Audit:

Verify the operating system implements certificate status checking for PKI authentication.

Check to see if Online Certificate Status Protocol (OCSP) is enabled on the system with the following command:

```
# grep cert_policy /etc/pam_pkcs11/pam_pkcs11.conf | grep -v "^#"

cert_policy = ca, ocsp_on, signature;
cert_policy = ca, ocsp_on, signature;
cert_policy = ca, ocsp_on, signature;
```

There should be at least three lines returned.

If "ocsp_on" is not present in all uncommented "cert_policy" lines in "/etc/pam_pkcs11/pam_pkcs11.conf", this is a finding.

Remediation:

Configure the operating system to do certificate status checking for PKI authentication.

Modify all of the "cert_policy" lines in "/etc/pam_pkcs11/pam_pkcs11.conf" to include "ocsp_on".

Additional Information:

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)

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 Accept 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 verify Personal Identity Verification-compliant credentials.

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

1.242 OL07-00-041010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must be configured so that all wireless network adapters are disabled.

```
GROUP ID: V-221898
RULE ID: SV-221898r971547
```

Rationale:

The use of wireless networking can introduce many different attack vectors into the organization's network. Common attack vectors such as malicious association and ad hoc networks will allow an attacker to spoof a wireless access point (AP), allowing validated systems to connect to the malicious AP, and enabling the attacker to monitor and record network traffic. These malicious APs can also serve to create a man-in-the-middle attack, or be used to create a denial of service to valid network resources.

Audit:

Verify that there are no wireless interfaces configured on the system.

This is N/A for systems that do not have wireless network adapters.

Check for the presence of active wireless interfaces with the following command:

```
# nmcli device
DEVICE TYPE STATE
eth0 ethernet connected
wlp3s0 wifi disconnected
lo loopback unmanaged
```

If a wireless interface is configured and its use on the system is not documented with 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 wifi off
```

Additional Information:

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)

1.243 OL07-00-910055 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Oracle Linux operating system must protect audit information from unauthorized read, modification, or deletion.

```
GROUP ID: V-221899
RULE ID: SV-221899r958434
```

Rationale:

If audit information were to become compromised, then forensic analysis and discovery of the true source of potentially malicious system activity is impossible to achieve.

To ensure the veracity of audit information, the operating system must protect audit information from unauthorized modification.

Audit information includes all information (e.g., audit records, audit settings, audit reports) needed to successfully audit information system activity.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029, SRG-OS-000206-GPOS-00084

Audit:

Verify the operating system audit records have proper permissions and ownership.

List the full permissions and ownership of the audit log files with the following command.

```
# ls -la /var/log/audit
total 4512
drwx------. 2 root root 23 Apr 25 16:53 .
drwxr-xr-x. 17 root root 4096 Aug 9 13:09 ..
-rw-------. 1 root root 8675309 Aug 9 12:54 audit.log
```

Audit logs must be mode 0600 or less permissive.

If any are more permissive, this is a finding.

The owner and group owner of all audit log files must both be "root". If any other owner or group owner is listed, this is a finding.

Remediation:

Change the mode of the audit log files with the following command:

```
# chmod 0600 [audit_file]
```

Change the owner and group owner of the audit log files with the following command:

```
# chown root:root [audit_file]
```

Additional Information:

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

- NIST SP 800-53::SI-11 c
- NIST SP 800-53A::SI-11.1 (iv)
- NIST SP 800-53 Revision 4::SI-11 b
- NIST SP 800-53 Revision 5::SI-11 b

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	OL07-00-010010 (Manual)	☐	☐
1.2	OL07-00-010019 (Manual)	☐	☐
1.3	OL07-00-010020 (Manual)	☐	☐
1.4	OL07-00-010030 (Manual)	☐	☐
1.5	OL07-00-010040 (Manual)	☐	☐
1.6	OL07-00-010050 (Manual)	☐	☐
1.7	OL07-00-010060 (Manual)	☐	☐
1.8	OL07-00-010062 (Manual)	☐	☐
1.9	OL07-00-010061 (Manual)	☐	☐
1.10	OL07-00-010063 (Manual)	☐	☐
1.11	OL07-00-010070 (Manual)	☐	☐
1.12	OL07-00-010081 (Manual)	☐	☐
1.13	OL07-00-010082 (Manual)	☐	☐
1.14	OL07-00-010100 (Manual)	☐	☐
1.15	OL07-00-010101 (Manual)	☐	☐
1.16	OL07-00-010110 (Manual)	☐	☐
1.17	OL07-00-010118 (Manual)	☐	☐
1.18	OL07-00-010119 (Manual)	☐	☐
1.19	OL07-00-010120 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	OL07-00-010130 (Manual)	☐	☐
1.21	OL07-00-010140 (Manual)	☐	☐
1.22	OL07-00-010150 (Manual)	☐	☐
1.23	OL07-00-010160 (Manual)	☐	☐
1.24	OL07-00-010170 (Manual)	☐	☐
1.25	OL07-00-010180 (Manual)	☐	☐
1.26	OL07-00-010190 (Manual)	☐	☐
1.27	OL07-00-010199 (Manual)	☐	☐
1.28	OL07-00-010200 (Manual)	☐	☐
1.29	OL07-00-010210 (Manual)	☐	☐
1.30	OL07-00-010220 (Manual)	☐	☐
1.31	OL07-00-010230 (Manual)	☐	☐
1.32	OL07-00-010250 (Manual)	☐	☐
1.33	OL07-00-010240 (Manual)	☐	☐
1.34	OL07-00-010260 (Manual)	☐	☐
1.35	OL07-00-010271 (Manual)	☐	☐
1.36	OL07-00-010280 (Manual)	☐	☐
1.37	OL07-00-010290 (Manual)	☐	☐
1.38	OL07-00-010291 (Manual)	☐	☐
1.39	OL07-00-010300 (Manual)	☐	☐
1.40	OL07-00-010310 (Manual)	☐	☐
1.41	OL07-00-010320 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	OL07-00-010330 (Manual)	☐	☐
1.43	OL07-00-010339 (Manual)	☐	☐
1.44	OL07-00-010340 (Manual)	☐	☐
1.45	OL07-00-010341 (Manual)	☐	☐
1.46	OL07-00-010342 (Manual)	☐	☐
1.47	OL07-00-010343 (Manual)	☐	☐
1.48	OL07-00-010344 (Manual)	☐	☐
1.49	OL07-00-010350 (Manual)	☐	☐
1.50	OL07-00-010375 (Manual)	☐	☐
1.51	OL07-00-010430 (Manual)	☐	☐
1.52	OL07-00-010440 (Manual)	☐	☐
1.53	OL07-00-010450 (Manual)	☐	☐
1.54	OL07-00-010460 (Manual)	☐	☐
1.55	OL07-00-010470 (Manual)	☐	☐
1.56	OL07-00-010481 (Manual)	☐	☐
1.57	OL07-00-010482 (Manual)	☐	☐
1.58	OL07-00-010483 (Manual)	☐	☐
1.59	OL07-00-010491 (Manual)	☐	☐
1.60	OL07-00-010492 (Manual)	☐	☐
1.61	OL07-00-010500 (Manual)	☐	☐
1.62	OL07-00-020000 (Manual)	☐	☐
1.63	OL07-00-020010 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	OL07-00-020020 (Manual)	☐	☐
1.65	OL07-00-020021 (Manual)	☐	☐
1.66	OL07-00-020022 (Manual)	☐	☐
1.67	OL07-00-020023 (Manual)	☐	☐
1.68	OL07-00-020028 (Manual)	☐	☐
1.69	OL07-00-020029 (Manual)	☐	☐
1.70	OL07-00-020030 (Manual)	☐	☐
1.71	OL07-00-020040 (Manual)	☐	☐
1.72	OL07-00-020050 (Manual)	☐	☐
1.73	OL07-00-020060 (Manual)	☐	☐
1.74	OL07-00-020100 (Manual)	☐	☐
1.75	OL07-00-020101 (Manual)	☐	☐
1.76	OL07-00-020110 (Manual)	☐	☐
1.77	OL07-00-020111 (Manual)	☐	☐
1.78	OL07-00-020200 (Manual)	☐	☐
1.79	OL07-00-020210 (Manual)	☐	☐
1.80	OL07-00-020220 (Manual)	☐	☐
1.81	OL07-00-020230 (Manual)	☐	☐
1.82	OL07-00-020231 (Manual)	☐	☐
1.83	OL07-00-020240 (Manual)	☐	☐
1.84	OL07-00-020250 (Manual)	☐	☐
1.85	OL07-00-020260 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.86	OL07-00-020270 (Manual)	☐	☐
1.87	OL07-00-020300 (Manual)	☐	☐
1.88	OL07-00-020310 (Manual)	☐	☐
1.89	OL07-00-020320 (Manual)	☐	☐
1.90	OL07-00-020330 (Manual)	☐	☐
1.91	OL07-00-020610 (Manual)	☐	☐
1.92	OL07-00-020620 (Manual)	☐	☐
1.93	OL07-00-020630 (Manual)	☐	☐
1.94	OL07-00-020640 (Manual)	☐	☐
1.95	OL07-00-020650 (Manual)	☐	☐
1.96	OL07-00-020660 (Manual)	☐	☐
1.97	OL07-00-020670 (Manual)	☐	☐
1.98	OL07-00-020680 (Manual)	☐	☐
1.99	OL07-00-020690 (Manual)	☐	☐
1.100	OL07-00-020700 (Manual)	☐	☐
1.101	OL07-00-020710 (Manual)	☐	☐
1.102	OL07-00-020720 (Manual)	☐	☐
1.103	OL07-00-020730 (Manual)	☐	☐
1.104	OL07-00-020900 (Manual)	☐	☐
1.105	OL07-00-021000 (Manual)	☐	☐
1.106	OL07-00-021010 (Manual)	☐	☐
1.107	OL07-00-021020 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.108	OL07-00-021021 (Manual)	☐	☐
1.109	OL07-00-021024 (Manual)	☐	☐
1.110	OL07-00-021030 (Manual)	☐	☐
1.111	OL07-00-021031 (Manual)	☐	☐
1.112	OL07-00-021040 (Manual)	☐	☐
1.113	OL07-00-021100 (Manual)	☐	☐
1.114	OL07-00-021110 (Manual)	☐	☐
1.115	OL07-00-021120 (Manual)	☐	☐
1.116	OL07-00-021300 (Manual)	☐	☐
1.117	OL07-00-021310 (Manual)	☐	☐
1.118	OL07-00-021320 (Manual)	☐	☐
1.119	OL07-00-021330 (Manual)	☐	☐
1.120	OL07-00-021340 (Manual)	☐	☐
1.121	OL07-00-021350 (Manual)	☐	☐
1.122	OL07-00-021600 (Manual)	☐	☐
1.123	OL07-00-021610 (Manual)	☐	☐
1.124	OL07-00-021620 (Manual)	☐	☐
1.125	OL07-00-021700 (Manual)	☐	☐
1.126	OL07-00-021710 (Manual)	☐	☐
1.127	OL07-00-030000 (Manual)	☐	☐
1.128	OL07-00-030010 (Manual)	☐	☐
1.129	OL07-00-030201 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.130	OL07-00-030210 (Manual)	☐	☐
1.131	OL07-00-030211 (Manual)	☐	☐
1.132	OL07-00-030300 (Manual)	☐	☐
1.133	OL07-00-030310 (Manual)	☐	☐
1.134	OL07-00-030320 (Manual)	☐	☐
1.135	OL07-00-030321 (Manual)	☐	☐
1.136	OL07-00-030330 (Manual)	☐	☐
1.137	OL07-00-030340 (Manual)	☐	☐
1.138	OL07-00-030350 (Manual)	☐	☐
1.139	OL07-00-030360 (Manual)	☐	☐
1.140	OL07-00-030370 (Manual)	☐	☐
1.141	OL07-00-030410 (Manual)	☐	☐
1.142	OL07-00-030440 (Manual)	☐	☐
1.143	OL07-00-030510 (Manual)	☐	☐
1.144	OL07-00-030560 (Manual)	☐	☐
1.145	OL07-00-030570 (Manual)	☐	☐
1.146	OL07-00-030580 (Manual)	☐	☐
1.147	OL07-00-030590 (Manual)	☐	☐
1.148	OL07-00-030610 (Manual)	☐	☐
1.149	OL07-00-030620 (Manual)	☐	☐
1.150	OL07-00-030630 (Manual)	☐	☐
1.151	OL07-00-030640 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.152	OL07-00-030650 (Manual)	☐	☐
1.153	OL07-00-030660 (Manual)	☐	☐
1.154	OL07-00-030670 (Manual)	☐	☐
1.155	OL07-00-030680 (Manual)	☐	☐
1.156	OL07-00-030690 (Manual)	☐	☐
1.157	OL07-00-030700 (Manual)	☐	☐
1.158	OL07-00-030710 (Manual)	☐	☐
1.159	OL07-00-030720 (Manual)	☐	☐
1.160	OL07-00-030740 (Manual)	☐	☐
1.161	OL07-00-030750 (Manual)	☐	☐
1.162	OL07-00-030760 (Manual)	☐	☐
1.163	OL07-00-030770 (Manual)	☐	☐
1.164	OL07-00-030780 (Manual)	☐	☐
1.165	OL07-00-030800 (Manual)	☐	☐
1.166	OL07-00-030805 (Manual)	☐	☐
1.167	OL07-00-030810 (Manual)	☐	☐
1.168	OL07-00-030819 (Manual)	☐	☐
1.169	OL07-00-030820 (Manual)	☐	☐
1.170	OL07-00-030830 (Manual)	☐	☐
1.171	OL07-00-030840 (Manual)	☐	☐
1.172	OL07-00-030870 (Manual)	☐	☐
1.173	OL07-00-030871 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.174	OL07-00-030872 (Manual)	☐	☐
1.175	OL07-00-030873 (Manual)	☐	☐
1.176	OL07-00-030874 (Manual)	☐	☐
1.177	OL07-00-030910 (Manual)	☐	☐
1.178	OL07-00-031000 (Manual)	☐	☐
1.179	OL07-00-031010 (Manual)	☐	☐
1.180	OL07-00-032000 (Manual)	☐	☐
1.181	OL07-00-040000 (Manual)	☐	☐
1.182	OL07-00-040100 (Manual)	☐	☐
1.183	OL07-00-040110 (Manual)	☐	☐
1.184	OL07-00-040160 (Manual)	☐	☐
1.185	OL07-00-040170 (Manual)	☐	☐
1.186	OL07-00-040180 (Manual)	☐	☐
1.187	OL07-00-040190 (Manual)	☐	☐
1.188	OL07-00-040200 (Manual)	☐	☐
1.189	OL07-00-040201 (Manual)	☐	☐
1.190	OL07-00-040300 (Manual)	☐	☐
1.191	OL07-00-040310 (Manual)	☐	☐
1.192	OL07-00-040320 (Manual)	☐	☐
1.193	OL07-00-040330 (Manual)	☐	☐
1.194	OL07-00-040340 (Manual)	☐	☐
1.195	OL07-00-040350 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.196	OL07-00-040360 (Manual)	☐	☐
1.197	OL07-00-040370 (Manual)	☐	☐
1.198	OL07-00-040380 (Manual)	☐	☐
1.199	OL07-00-040390 (Manual)	☐	☐
1.200	OL07-00-040400 (Manual)	☐	☐
1.201	OL07-00-040410 (Manual)	☐	☐
1.202	OL07-00-040420 (Manual)	☐	☐
1.203	OL07-00-040430 (Manual)	☐	☐
1.204	OL07-00-040440 (Manual)	☐	☐
1.205	OL07-00-040450 (Manual)	☐	☐
1.206	OL07-00-040460 (Manual)	☐	☐
1.207	OL07-00-040470 (Manual)	☐	☐
1.208	OL07-00-040500 (Manual)	☐	☐
1.209	OL07-00-040510 (Manual)	☐	☐
1.210	OL07-00-040520 (Manual)	☐	☐
1.211	OL07-00-040530 (Manual)	☐	☐
1.212	OL07-00-040540 (Manual)	☐	☐
1.213	OL07-00-040550 (Manual)	☐	☐
1.214	OL07-00-040600 (Manual)	☐	☐
1.215	OL07-00-040610 (Manual)	☐	☐
1.216	OL07-00-040611 (Manual)	☐	☐
1.217	OL07-00-040612 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.218	OL07-00-040620 (Manual)	☐	☐
1.219	OL07-00-040630 (Manual)	☐	☐
1.220	OL07-00-040640 (Manual)	☐	☐
1.221	OL07-00-040641 (Manual)	☐	☐
1.222	OL07-00-040650 (Manual)	☐	☐
1.223	OL07-00-040660 (Manual)	☐	☐
1.224	OL07-00-040670 (Manual)	☐	☐
1.225	OL07-00-040680 (Manual)	☐	☐
1.226	OL07-00-040690 (Manual)	☐	☐
1.227	OL07-00-040700 (Manual)	☐	☐
1.228	OL07-00-040710 (Manual)	☐	☐
1.229	OL07-00-040711 (Manual)	☐	☐
1.230	OL07-00-040712 (Manual)	☐	☐
1.231	OL07-00-040720 (Manual)	☐	☐
1.232	OL07-00-040730 (Manual)	☐	☐
1.233	OL07-00-040740 (Manual)	☐	☐
1.234	OL07-00-040750 (Manual)	☐	☐
1.235	OL07-00-040800 (Manual)	☐	☐
1.236	OL07-00-040810 (Manual)	☐	☐
1.237	OL07-00-040820 (Manual)	☐	☐
1.238	OL07-00-040830 (Manual)	☐	☐
1.239	OL07-00-041001 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.240	OL07-00-041002 (Manual)	☐	☐
1.241	OL07-00-041003 (Manual)	☐	☐
1.242	OL07-00-041010 (Manual)	☐	☐
1.243	OL07-00-910055 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 22, 2025	1.0.0	Initial CIS Release