CIS Center for Internet Security®

CIS Benchmarks™

CIS SUSE Linux Enterprise Server 15 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

SUSE Linux Enterprise Server 15 Secure Technical Implementation Guide (STIG)

Version: 2 Release: 4 Benchmark

Date: 02 Apr 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate SUSE Linux Enterprise Server 15 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 SUSE Linux Enterprise Server 15

Recommendations

1 STIG RULES

SUSE Linux Enterprise Server 15

SUSE Linux Enterprise Server 15 Secure Technical Implementation Guide (STIG)

Version: 2 Release: 4 Benchmark

Date: 02 Apr 2025

CLASSIFICATION unclassified

1.1 SLES-15-010000 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The SUSE operating system must be a vendor-supported release.

```
GROUP ID: V-234800
RULE ID: SV-234800r991589
```

Rationale:

A SUSE 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 SUSE operating system is a vendor-supported release.

Use the following command to verify the SUSE operating system is a vendor-supported release:

```
cat /etc/os-release

NAME="SLES"
VERSION="15"
```

Or any SUSE Linux Enterprise 15 Service Pack follow up release.

```
NAME="SLES"
VERSION="15-SPx"
```

Current End of Life for SLES 15 General Support is 31 Jul 2028 and Long-term Support is until 31 Jul 2031.

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

Remediation:

Upgrade the SUSE operating system to a version supported by the vendor. If the system is not registered with the SUSE Customer Center, register the system against the correct subscription.

If the system requires Long-Term Service Pack Support (LTSS), obtain the correct LTSS subscription for the system.

Additional Information:

CCI-001230 Incorporate flaw remediation into the organizational configuration management process.

- NIST SP 800-53::SI-2 c
- NIST SP 800-53A::SI-2.1 (iv)
- NIST SP 800-53 Revision 4::SI-2 d
- NIST SP 800-53 Revision 5::SI-2 d

1.2 SLES-15-010010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Vendor-packaged SUSE operating system security patches and updates must be installed and up to date.

```
GROUP ID: V-234802
RULE ID: SV-234802r991589
```

Rationale:

Timely patching is critical for maintaining the operational availability, confidentiality, and integrity of information technology (IT) systems. However, failure to keep SUSE operating system and application software patched is a common mistake made by IT professionals. New patches are released frequently, and it is often difficult for even experienced System Administrators (SAs) to keep abreast of all the new patches. When new weaknesses in a SUSE 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 SUSE operating system security patches and updates are installed and up to date.

Note: Updates are required to be applied with a frequency determined by the site or Program Management Office (PMO).

Check for required SUSE operating system patches and updates with the following command:

```
sudo zypper patch-check

0 patches needed (0 security patches)
```

If the patch repository data is corrupt, check that the available package security updates have been installed on the system with the following command:

```
cut -d "|" -f 1-4 -s --output-delimiter " | " /var/log/zypp/history | grep -v
" radd "

2016-12-14 11:59:36 | install | libapparmor1-32bit | 2.8.0-2.4.1
2016-12-14 11:59:36 | install | pam_apparmor | 2.8.0-2.4.1
2016-12-14 11:59:36 | install | pam_apparmor-32bit | 2.8.0-2.4.1
```

If the SUSE operating system has not been patched within the site or PMO frequency, this is a finding.

Remediation:

Install the applicable SUSE operating system patches available from SUSE by running the following command:

```
sudo zypper patch
```

Additional Information:

CCI-001227 Correct system flaws.

- NIST SP 800-53::SI-2 a
- NIST SP 800-53A::SI-2.1 (i)
- NIST SP 800-53 Revision 4::SI-2 a
- NIST SP 800-53 Revision 5::SI-2 a

1.3 SLES-15-010020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must display the Standard Mandatory DOD Notice and Consent Banner before granting access via local console.

```
GROUP ID: V-234803
RULE ID: SV-234803r958390
```

Rationale:

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

The banner must be acknowledged by the user prior to allowing the user access to the SUSE operating system. This provides assurance that the user has seen the message and accepted the conditions for access. If the consent banner is not acknowledged by the user, DOD will not be in compliance with system use notifications required by law.

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 SUSE operating system:

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

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

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

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

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

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

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

Audit:

Verify the SUSE operating system displays the Standard Mandatory DOD Notice and Consent Banner before granting access to the system via local console.

Check the "motd" (message of the day) file to verify that it contains the DOD required banner text:

```
more /etc/issue
```

The output must display the following DOD-required banner 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 output does not display the correct banner text, this is a finding.

Remediation:

Configure the SUSE operating system to display the Standard Mandatory DOD Notice and Consent Banner before granting access to the system via local console by performing the following tasks:

Edit the "motd" file and replace the default text inside with the Standard Mandatory DOD banner 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."
```

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

1.4 SLES-15-010030 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The SUSE operating system must not have the vsftpd package installed if not required for operational support.

```
GROUP ID: V-234804
RULE ID: SV-234804r987796
```

Rationale:

It is detrimental for SUSE 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.

SUSE 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 and functions).

Examples of nonessential 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.

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

Audit:

Verify the vsftpd package is not installed on the SUSE operating system.

Check that the vsftpd package is not installed on the SUSE operating system by running the following command:

```
zypper info vsftpd | grep Installed
```

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:

```
sudo zypper remove vsftpd
```

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)

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

1.5 SLES-15-010040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must display the Standard Mandatory DOD Notice and Consent Banner before granting access via SSH.

```
GROUP ID: V-234805
RULE ID: SV-234805r958390
```

Rationale:

Display of a standardized and approved use notification before granting access to the SUSE 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 SUSE operating systems that can accommodate banners of 1300 characters:

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

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

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

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

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

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

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

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

Audit:

Verify the SUSE operating system displays the Standard Mandatory DOD Notice and Consent Banner before granting access to the system via SSH.

Check the issue file to verify it contains one of the DOD required banners. If it does not, this is a finding.

```
more /etc/issue
```

The output must display the following DOD-required banner 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 output does not display the banner text, this is a finding.

Check the banner setting for sshd_config:

```
sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' | tr
'\n' ' ' | xargs sudo grep -iH '^\s*banner'

Banner /etc/issue
```

If "Banner" is not set to "/etc/issue", this is a finding.

Remediation:

Configure the SUSE operating system to display the Standard Mandatory DOD Notice and Consent Banner before granting access to the system by running the following commands:

Edit the "sshd_config" file and edit the Banner flag to be the following:

```
Banner /etc/issue/
```

Restart the sshd daemon:

```
sudo systemctl restart sshd.service
```

To configure the system logon banner, edit the "/etc/issue" file. Replace the default text inside with the Standard Mandatory DOD banner 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."
```

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-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

1.6 SLES-15-010050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must display the Standard Mandatory DoD Notice and Consent Banner until users acknowledge the usage conditions and take explicit actions to log on for further access to the local graphical user interface (GUI).

```
GROUP ID: V-234806
RULE ID: SV-234806r958390
```

Rationale:

The SUSE operating system must display the Standard Mandatory DoD Notice and Consent Banner until users acknowledge the usage conditions and take explicit actions to log on for further access to the local graphical user interface (GUI).

Satisfies: SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007

Audit:

Verify the SUSE operating system displays the Standard Mandatory DoD Notice and Consent Banner until users acknowledge the usage conditions and take explicit actions to log on via the local GUI.

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

Check the configuration by running the following command:

```
more /etc/gdm/Xsession
```

The beginning of the file must contain the following text immediately after (#!/bin/sh):

```
if ! zenity --text-info \
--title "Consent" \
--filename=/etc/gdm/banner \
--no-markup \
--checkbox="Accept." 10 10; then
sleep 1;
exit 1;
fi
```

If the beginning of the file does not contain the above text immediately after the line (#!/bin/sh), this is a finding.

Remediation:

Configure the SUSE operating system to display the Standard Mandatory DoD Notice and Consent Banner until users acknowledge the usage conditions and take explicit actions to log on for further access.

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

Edit the file "/etc/gdm/Xsession".

Add the following content to the file "/etc/gdm/Xsession" below the line #!/bin/sh:

```
if ! zenity --text-info \
--title "Consent" \
--filename=/etc/gdm/banner \
--no-markup \
--checkbox="Accept." 10 10; then
sleep 1;
exit 1;
fi
```

Save the file "/etc/gdm/Xsession".

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

1.7 SLES-15-010080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must display a banner before granting local or remote access to the system via a graphical user logon.

```
GROUP ID: V-234808
RULE ID: SV-234808r958586
```

Rationale:

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

The banner must be acknowledged by the user prior to allowing the user access to the SUSE operating system. This provides assurance that the user has seen the message and accepted the conditions for access. If the consent banner is not acknowledged by the user, DoD will not be in compliance with system use notifications required by law.

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 SUSE operating system:

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

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

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

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

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

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

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

Audit:

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

Verify the SUSE operating system displays a banner before local or remote access to the system via a graphical user logon.

Check that the SUSE operating system displays a banner at the logon screen by performing the following command:

```
grep banner-message-enable /etc/dconf/db/gdm.d/*
banner-message-enable=true
cat /etc/dconf/profile/gdm
user-db:user
system-db:gdm
file-db:/usr/share/gdm/greeter-dconf-defaults
```

If "banner-message-enable" is set to "false" or is missing completely, this is a finding.

Remediation:

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

Configure the SUSE operating system to display a banner before local or remote access to the system via a graphical user logon.

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

```
sudo mkdir -p /etc/dconf/db/gdm.d
sudo touch /etc/dconf/db/gdm.d/01-banner-message
```

Add the following content into /etc/dconf/profile/gdm:

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

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

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

Update the system databases:

```
sudo dconf update
```

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

Additional Information:

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

1.8 SLES-15-010090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-234809
RULE ID: SV-234809r958586
```

Rationale:

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

The banner must be acknowledged by the user prior to allowing the user access to the SUSE operating system. This provides assurance that the user has seen the message and accepted the conditions for access. If the consent banner is not acknowledged by the user, DoD will not be in compliance with system use notifications required by law.

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 SUSE operating system:

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

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

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

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

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

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

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

Audit:

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

Verify the SUSE operating system displays the approved Standard Mandatory DoD Notice before granting local or remote access to the system via a graphical user logon.

Check that the SUSE operating system displays the exact approved Standard Mandatory DoD Notice and Consent Banner text by performing the following command:

```
grep banner-message-text /etc/dconf/db/gdm.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 GUI.

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

Remediation:

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

Configure the SUSE operating system to display the approved Standard Mandatory DoD Notice before granting local or remote access to the system via a graphical user logon.

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

```
sudo touch /etc/dconf/db/gdm.d/01-banner-message
```

Add the following lines to the "[org/gnome/login-screen]" section of the "dconf/db/gdm.d/01-banner-message" file:

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

Run the following command to update the database:

```
sudo dconf update
```

Additional Information:

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

1.9 SLES-15-010060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system file /etc/gdm/banner must contain the Standard Mandatory DoD Notice and Consent banner text.

```
GROUP ID: V-234807
RULE ID: SV-234807r958392
```

Rationale:

The banner must be acknowledged by the user prior to allowing the user access to the SUSE operating system. This provides assurance that the user has seen the message and accepted the conditions for access. If the consent banner is not acknowledged by the user, DoD will not be in compliance with system use notifications required by law.

To establish acceptance of the application usage policy, a click-through banner at system logon is required. The system must prevent further activity until the user executes a positive action to manifest agreement by clicking on a box indicating "OK".

Audit:

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

Verify the SUSE operating system file "/etc/gdm/banner" contains the Standard Mandatory DoD Notice and Consent Banner text by running the following command:

```
more /etc/gdm/banner
```

If the file does not contain the following text, this is a finding.

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

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

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

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

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

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

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

Remediation:

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

Configure the SUSE operating system file "/etc/gdm/banner" to contain the Standard Mandatory DoD Notice and Consent Banner by running the following commands:

```
sudo vi /etc/gdm/banner
```

Add the following information to the file:

```
"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-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

1.10 SLES-15-010100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must be able to lock the graphical user interface (GUI).

```
GROUP ID: V-234810
RULE ID: SV-234810r1009609
```

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 SUSE operating system allows the user to lock the GUI.

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

Run the following command:

```
sudo gsettings get org.gnome.desktop.lockdown disable-lock-screen
```

If the result is "true", this is a finding.

Remediation:

Note: If the system does not have a graphical user interface installed, this requirement is Not Applicable. This command must be run from an X11 session; otherwise, the command will not work correctly.

Configure the SUSE operating system to allow the user to lock the GUI.

Run the following command to configure the SUSE operating system to allow the user to lock the GUI:

```
sudo gsettings set org.gnome.desktop.lockdown disable-lock-screen false
```

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-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

CCI-000060 Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

- NIST SP 800-53::AC-11 (1)
- NIST SP 800-53A::AC-11 (1).1
- NIST SP 800-53 Revision 4::AC-11 (1)
- NIST SP 800-53 Revision 5::AC-11 (1)

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

1.11 SLES-15-010110 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The SUSE operating system must utilize vlock to allow for session locking.

```
GROUP ID: V-234811
RULE ID: SV-234811r1009610
```

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, SRG-OS-000031-GPOS-00012

Audit:

Check that the SUSE operating system has the "vlock" package installed by running the following command:

```
zypper search --installed-only --match-exact --provides vlock
```

If the command outputs "no matching items found", this is a finding.

Remediation:

Allow users to lock the console by installing the "kbd" package using zypper:

```
sudo zypper install kbd
```

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-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

CCI-000060 Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

- NIST SP 800-53::AC-11 (1)
- NIST SP 800-53A::AC-11 (1).1
- NIST SP 800-53 Revision 4::AC-11 (1)
- NIST SP 800-53 Revision 5::AC-11 (1)

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

1.12 SLES-15-010120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must initiate a session lock after a 15-minute period of inactivity for the graphical user interface (GUI).

```
GROUP ID: V-234812
RULE ID: SV-234812r958402
```

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 users to manually lock their SUSE operating system session prior to vacating the vicinity, the SUSE operating system needs to be able to identify when a user's session has idled and take action to initiate the session lock.

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

Audit:

Verify the SUSE operating system initiates a session lock after a 15-minute period of inactivity via the GUI by running the following command:

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

```
sudo gsettings get org.gnome.desktop.session idle-delay

uint32 900
```

If the command does not return a value less than or equal to "900", this is a finding.

Remediation:

Configure the SUSE operating system to initiate a session lock after a 15-minute period of inactivity of the GUI by running the following command:

Note: If the system does not have a graphical user interface installed, this requirement is Not Applicable. This command must be run from an X11 session, otherwise the command will not work correctly.

```
sudo gsettings set org.gnome.desktop.session idle-delay 900
```

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 SLES-15-010130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must initiate a session lock after a 10-minute period of inactivity.

```
GROUP ID: V-234813
RULE ID: SV-234813r1009561
```

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 users to manually lock their SUSE operating system session prior to vacating the vicinity, the SUSE operating system needs to be able to identify when a user's session has idled and take action to initiate the session lock.

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

Audit:

Verify the SUSE operating system must initiate a session logout after a 10-minute period of inactivity for all connection types.

Check the proper script exists to kill an idle session after a 10-minute period of inactivity with the following command:

```
cat /etc/profile.d/autologout.sh
TMOUT=600
readonly TMOUT
export TMOUT
```

If the file "/etc/profile.d/autologout.sh" does not exist or the output from the function call is not the same, this is a finding.

Remediation:

Configure the SUSE operating system to initiate a session lock after a 10-minute period of inactivity by modifying or creating (if it does not already exist) the "/etc/profile.d/autologout.sh" file and add the following lines to it:

```
TMOUT=600
readonly TMOUT
export TMOUT
```

Set the proper permissions for the "/etc/profile.d/autologout.sh" file with the following command:

```
sudo chmod +x /etc/profile.d/autologout.sh
```

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 SLES-15-010140 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The SUSE operating system must conceal, via the session lock, information previously visible on the display with a publicly viewable image in the graphical user interface (GUI).

```
GROUP ID: V-234814
RULE ID: SV-234814r958404
```

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 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 SUSE operating system session lock event must include an obfuscation of the display screen to prevent other users from reading what was previously displayed.

Publicly viewable images can include static or dynamic images, such as patterns used with screen savers, photographic images, solid colors, a clock, a battery life indicator, or a blank screen, with the additional caveat that none of the images conveys sensitive information.

Audit:

Verify the SUSE operating system conceals via the session lock information previously visible on the display with a publicly viewable image in the GUI.

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

Check that the lock screen is set to a publicly viewable image by running the following command:

```
sudo gsettings get org.gnome.desktop.screensaver picture-uri
'file:///usr/share/wallpapers/SLE-default-static.xml'
```

If nothing is returned or "org.gnome.desktop.screensaver" is not set, this is a finding.

Remediation:

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

Configure the SUSE operating system to use a publically viewable image by finding the Settings menu and then navigate to the Background selection section:

- Click "Activities" on the top left.
- Click "Show Applications" at the bottom of the Activities menu.
- Click the "Settings" icon.
- Click "Background" from left hand menu.
- Select image and set the Lock Screen image to the user's choice.
- Exit Settings Dialog.

Additional Information:

CCI-000060 Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

- NIST SP 800-53::AC-11 (1)
- NIST SP 800-53A::AC-11 (1).1
- NIST SP 800-53 Revision 4::AC-11 (1)
- NIST SP 800-53 Revision 5::AC-11 (1)

1.15 SLES-15-010150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must log SSH connection attempts and failures to the server.

```
GROUP ID: V-234815
RULE ID: SV-234815r958406
```

Rationale:

Remote access services, such as those providing remote access to network devices and information systems, which lack automated monitoring capabilities, increase risk and make remote user access management difficult at best.

Remote access is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Automated monitoring of remote access sessions allows organizations to detect cyber attacks and also ensure ongoing compliance with remote access policies by auditing connection activities of remote access capabilities, such as Remote Desktop Protocol (RDP), on a variety of information system components (e.g., servers, workstations, notebook computers, smartphones, and tablets).

Audit:

Verify SSH is configured to verbosely log connection attempts and failed logon attempts to the SUSE operating system.

Check that the SSH daemon configuration verbosely logs connection attempts and failed logon attempts to the server with the following command:

```
sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' | tr
'\n' ' ' | xargs sudo grep -iH '^\s*loglevel'
```

The output message must contain the following text:

```
LogLevel VERBOSE
```

If the output message does not contain "VERBOSE", the LogLevel keyword is missing, or the line is commented out, this is a finding.

Remediation:

Configure SSH to verbosely log connection attempts and failed logon attempts to the SUSE operating system.

Add or update the following line in the "/etc/ssh/sshd_config" file:

```
LogLevel VERBOSE
```

The SSH service will need to be restarted in order for the changes to take effect.

Additional Information:

CCI-000067 Employ automated mechanisms to monitor remote access methods.

- NIST SP 800-53::AC-17 (1)
- NIST SP 800-53A::AC-17 (1).1
- NIST SP 800-53 Revision 4::AC-17 (1)
- NIST SP 800-53 Revision 5::AC-17 (1)

1.16 SLES-15-010160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must implement DOD-approved encryption to protect the confidentiality of SSH remote connections.

```
GROUP ID: V-234816
RULE ID: SV-234816r958408
```

Rationale:

Without confidentiality protection mechanisms, unauthorized individuals may gain access to sensitive information via a remote access session.

Remote access is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Encryption provides a means to secure the remote connection to prevent unauthorized access to the data traversing the remote access connection (e.g., RDP), thereby providing a degree of confidentiality. The encryption strength of a mechanism is selected based on the security categorization of the information.

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-000125-GPOS-00065, SRG-OS-000250-GPOS-00093, SRG-OS-000393-GPOS-00173

Audit:

Verify the SUSE operating system implements DOD-approved encryption to protect the confidentiality of SSH remote connections.

Check the SSH daemon configuration for allowed ciphers with the following command:

```
sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' | tr
'\n' ' ' | xargs sudo grep -iH '^\s*ciphers'

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, or the "Ciphers" keyword is missing, this is a finding.

Remediation:

Edit the SSH daemon configuration (/etc/ssh/sshd_config) and remove any ciphers not starting with "aes" and remove any ciphers ending with "cbc". If necessary, add a "Ciphers" line:

```
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
```

Restart the SSH daemon:

```
sudo systemctl restart sshd.service
```

Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

1.17 SLES-15-010170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system, for PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.

```
GROUP ID: V-234817
RULE ID: SV-234817r1009611
```

Rationale:

Without path validation, an informed trust decision by the relying party cannot be made when presented with any certificate not already explicitly trusted.

A trust anchor is an authoritative entity represented via a public key and associated data. It is used in the context of public key infrastructures, X.509 digital certificates, and DNSSEC.

When there is a chain of trust, usually the top entity to be trusted becomes the trust anchor; it can be, for example, a Certification Authority (CA). A certification path starts with the subject certificate and proceeds through a number of intermediate certificates up to a trusted root certificate, typically issued by a trusted CA.

This requirement verifies that a certification path to an accepted trust anchor is used for certificate validation and that the path includes status information. Path validation is necessary for a relying party to make an informed trust decision when presented with any certificate not already explicitly trusted. Status information for certification paths includes certificate revocation lists or online certificate status protocol responses. Validation of the certificate status information is out of scope for this requirement.

Satisfies: SRG-OS-000066-GPOS-00034, SRG-OS-000384-GPOS-00167

Audit:

Verify the SUSE operating system for PKI-based authentication had valid certificates by constructing a certification path (which includes status information) to an accepted trust anchor.

Check that the certification path to an accepted trust anchor for multifactor authentication is implemented with the following command:

```
grep cert_policy /etc/pam_pkcs11/pam_pkcs11.conf

cert_policy = ca,oscp_on,signature,crl_auto;
```

If "cert_policy" is not set to include "ca", this is a finding.

Remediation:

Configure the SUSE operating system for PKI-based authentication to validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.

Modify all of the cert_policy lines in "/etc/pam_pkcs11/pam_pkcs11.conf" to include "ca":

```
cert_policy = ca,signature,oscp_on;
```

Note: Additional certificate validation polices are permitted.

Additional information on the configuration of multifactor authentication on the SUSE operating system can be found at https://www.suse.com/communities/blog/configuring-smart-card-authentication-suse-linux-enterprise/.

Additional Information:

CCI-000185 For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

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

CCI-004068 For public key-based authentication, implement a local cache of revocation data to support path discovery and validation.

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

CCI-001991 The information system, for PKI-based authentication, implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

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

1.18 SLES-15-010180 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The SUSE operating system must not have the telnet-server package installed.

```
GROUP ID: V-234818
RULE ID: SV-234818r987796
```

Rationale:

It is detrimental for SUSE 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.

SUSE 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 and functions).

Examples of nonessential 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.

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

Audit:

Verify the telnet-server package is not installed on the SUSE operating system.

Check that the telnet-server package is not installed on the SUSE operating system by running the following command:

```
zypper info telnet-server | grep Installed
```

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

Remediation:

Remove the telnet-server package from the SUSE operating system by running the following command:

```
sudo zypper remove telnet-server
```

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)

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

1.19 SLES-15-010190 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

SUSE operating systems with a basic input/output system (BIOS) must require authentication upon booting into single-user and maintenance modes.

```
GROUP ID: V-234819
RULE ID: SV-234819r958472
```

Rationale:

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

Access control policies include identity-based policies, role-based policies, and attribute-based policies. Access enforcement mechanisms include access control lists, access control matrices, and cryptography. These policies and mechanisms must be employed by the application to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, and domains) in the information system.

Audit:

Verify that the SUSE operating system has set an encrypted root password.

Note: If the system does not use a BIOS this requirement is Not Applicable.

Check that the encrypted password is set for root with the following command:

```
sudo cat /boot/grub2/grub.cfg | grep -i password

password_pbkdf2 root grub.pbkdf2.sha512.10000.VeryLongString
```

If the root password entry does not begin with "password_pbkdf2", this is a finding.

Remediation:

Note: If the system does not use a BIOS this requirement is Not Applicable.

Configure the SUSE operating system to encrypt the boot password.

Generate an encrypted (GRUB2) password for root with the following command:

```
grub2-mkpasswd-pbkdf2
Enter Password:
Reenter Password:
PBKDF2 hash of your password is
grub.pbkdf2.sha512.10000.MFU48934NJD84NF8NSD39993JDHF84NG
```

Using the hash from the output, modify the "/etc/grub.d/40_custom" file and add the following two lines to add a boot password for the root entry:

```
set superusers="root"
password_pbkdf2 root grub.pbkdf2.sha512.VeryLongString
```

Generate an updated "grub.conf" file with the new password using the following commands:

```
sudo grub2-mkconfig --output=/tmp/grub2.cfg
sudo mv /tmp/grub2.cfg /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

1.20 SLES-15-010200 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

SUSE operating systems with Unified Extensible Firmware Interface (UEFI) implemented must require authentication upon booting into single-user mode and maintenance.

```
GROUP ID: V-234820
RULE ID: SV-234820r958472
```

Rationale:

If the system allows a user to boot into single-user or maintenance mode without authentication, any user that invokes single-user or maintenance mode is granted privileged access to all system information.

Audit:

Verify that the SUSE operating system has set an encrypted root password.

Note: If the system does not use UEFI, this requirement is Not Applicable.

Check that the encrypted password is set for root with the following command:

```
sudo cat /boot/efi/EFI/sles/grub.cfg | grep -i password

password_pbkdf2 root grub.pbkdf2.sha512.10000.VeryLongString
```

If the root password entry does not begin with "password_pbkdf2", this is a finding.

Remediation:

Note: If the system does not use UEFI, this requirement is Not Applicable.

Configure the SUSE operating system to encrypt the boot password.

Generate an encrypted (GRUB2) password for root with the following command:

```
grub2-mkpasswd-pbkdf2
Enter Password:
Reenter Password:
PBKDF2 hash of your password is
grub.pbkdf2.sha512.10000.MFU48934NJD84NF8NSD39993JDHF84NG
```

Using the hash from the output, modify the "/etc/grub.d/40_custom" file and add the following two lines to add a boot password for the root entry:

```
set superusers="root"
password_pbkdf2 root grub.pbkdf2.sha512.VeryLongString
```

Generate an updated "grub.conf" file with the new password using the following commands:

```
sudo grub2-mkconfig --output=/tmp/grub2.cfg
sudo mv /tmp/grub2.cfg /boot/efi/EFI/sles/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

1.21 SLES-15-010220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services as defined in the Ports, Protocols, and Services Management (PPSM) Category Assignments List (CAL) and vulnerability assessments.

```
GROUP ID: V-234821
RULE ID: SV-234821r958480
```

Rationale:

To prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable or restrict unused or unnecessary physical and logical ports/protocols on information systems.

SUSE 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 SUSE 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 address authorized quality-of-life issues.

Satisfies: SRG-OS-000096-GPOS-00050, SRG-OS-000297-GPOS-00115, SRG-OS-000480-GPOS-00232

Audit:

Verify the SUSE operating system is configured to prohibit or restrict the use of functions, ports, protocols, and/or services as defined in the PPSM CAL and vulnerability assessments.

Check that the "firewalld.service" is enabled and running by running the following command:

```
systemctl status firewalld.service
 firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor
preset: disabled)
   Active: active (running) since Wed 2019-11-06 10:58:11 CET; 24h ago
     Docs: man:firewalld(1)
 Main PID: 1105 (firewalld)
    Tasks: 2 (limit: 4915)
   CGroup: /system.slice/firewalld.service
           ??1105 /usr/bin/python3 -Es /usr/sbin/firewalld --nofork --nopid
```

If the service is not enabled, this is a finding.

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

Check the firewall configuration for any unnecessary or prohibited functions, ports, protocols, and/or services by running the following command:

```
sudo firewall-cmd --list-all
```

Ask the System Administrator for the site or program PPSM Component Local Services Assessment (Component Local Services Assessment (CLSA). Verify the services allowed by the firewall match the PPSM CLSA.

If there are any additional ports, protocols, or services that are not included in the PPSM CLSA, this is a finding.

If there are any ports, protocols, or services that are prohibited by the PPSM CAL, this is a finding.

Remediation:

Configure the SUSE operating system is configured to prohibit or restrict the use of functions, ports, protocols, and/or services as defined in the PPSM CAL and vulnerability assessments.

Add/modify /etc/firewalld configuration files to comply with the PPSM CAL.

Enable the "firewalld.service" by running the following command:

```
sudo systemctl enable firewalld.service
```

Start the "firewalld.service" by running the following command:

```
sudo systemctl start firewalld.service
```

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)

1.22 SLES-15-010230 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must not have duplicate User IDs (UIDs) for interactive users.

```
GROUP ID: V-234822
RULE ID: SV-234822r958482
```

Rationale:

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

Interactive users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Interactive 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-000121-GPOS-00062

Audit:

Verify the SUSE operating system contains no duplicate UIDs for interactive users.

Check that the SUSE operating system contains no duplicate UIDs for interactive users by running the following command:

```
awk -F ":" 'list[$3]++{print $1, $3}' /etc/passwd
```

If output is produced, this is a finding.

Remediation:

Configure the SUSE operating system to contain no duplicate UIDs for interactive users.

Edit the file "/etc/passwd" and provide each interactive user account that has a duplicate UID with a unique UID.

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-000804 Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

- NIST SP 800-53::IA-8
- NIST SP 800-53A::IA-8.1
- NIST SP 800-53 Revision 4::IA-8
- NIST SP 800-53 Revision 5::IA-8

1.23 SLES-15-010240 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must disable the file system automounter unless required.

```
GROUP ID: V-234823
RULE ID: SV-234823r958498
```

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

Audit:

Verify the SUSE 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 SUSE operating system to disable the ability to automount devices.

Turn off the automount service with the following command:

```
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

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

1.24 SLES-15-010260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must employ FIPS 140-2 approved cryptographic hashing algorithm for system authentication (login.defs).

```
GROUP ID: V-234825
RULE ID: SV-234825r971535
```

Rationale:

Unapproved mechanisms that are used for authentication to the cryptographic module are not verified and therefore cannot be relied on to provide confidentiality or integrity, and DoD data may be compromised.

SUSE 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 that mechanisms used to access cryptographic modules use authentication that meets DoD requirements. This allows for Security Levels 1, 2, 3, or 4 for use on a general-purpose computing system.

Audit:

Verify the SUSE operating system requires that the "ENCRYPT_METHOD" value in "/etc/login.defs" is set to "SHA512".

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

```
grep "^ENCRYPT_METHOD " /etc/login.defs

ENCRYPT_METHOD SHA512
```

If "ENCRYPT_METHOD" is not set to "SHA512", if any values other that "SHA512" are configured, or if no output is produced, this is a finding.

Remediation:

Configure the SUSE operating system to require "ENCRYPT_METHOD" of "SHA512".

Edit the "/etc/login.defs" file with the following line:

```
ENCRYPT_METHOD SHA512
```

Additional Information:

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

1.25 SLES-15-010270 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system SSH daemon must be configured to only use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hash algorithms.

```
GROUP ID: V-234826
RULE ID: SV-234826r958510
```

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access (e.g., RDP) is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

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

The system will attempt to use the first hash presented by the client that matches the server list. Listing the values "strongest to weakest" is a method to ensure the use of the strongest hash available to secure the SSH connection.

Satisfies: SRG-OS-000125-GPOS-00065, SRG-OS-000394-GPOS-00174

Audit:

Verify the SUSE operating system SSH daemon is configured to only use MACs that employ FIPS 140-2 approved hashes.

Check that the SSH daemon is configured to only use MACs that employ FIPS 140-2 approved hashes with the following command:

```
sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' | tr
'\n' ' ' | xargs sudo grep -iH '^\s*macs'

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:

Configure the SUSE operating system SSH daemon to only use MACs that employ FIPS 140-2 approved hashes.

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" (The file might be named differently or be in a different location):

```
MACs hmac-sha2-512,hmac-sha2-256
```

Additional Information:

CCI-000877 Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions.

- NIST SP 800-53::MA-4 c
- NIST SP 800-53A::MA-4.1 (iv)
- NIST SP 800-53 Revision 4::MA-4 c
- NIST SP 800-53 Revision 5::MA-4 c

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)

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)

1.26 SLES-15-010280 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system SSH daemon must be configured with a timeout interval.

```
GROUP ID: V-234827
RULE ID: SV-234827r986464
```

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, deallocating associated TCP/IP address/port pairs at the SUSE operating system-level, and deallocating networking assignments at the application level if multiple application sessions are using a single SUSE operating system-level network connection. This does not mean that the SUSE operating system terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Satisfies: SRG-OS-000126-GPOS-00066, SRG-OS-000163-GPOS-00072, SRG-OS-000279-GPOS-00109

Audit:

Verify the SUSE operating system SSH daemon is configured to timeout idle sessions.

Check that the "ClientAliveInterval" parameter is set to a value of "600" with the following command:

```
sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' | tr
'\n' ' ' | xargs sudo grep -iH '^\s*clientaliveinterval'

ClientAliveInterval 600
```

If "ClientAliveInterval" is not set to "600" in "/etc/ssh/sshd_config", this is a finding.

Remediation:

Configure the SUSE operating system SSH daemon to timeout idle sessions.

Add or modify (to match exactly) the following line in the "/etc/ssh/sshd_config" file:

```
ClientAliveInterval 600
```

The SSH daemon must be restarted for any 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

1.27 SLES-15-010300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The sticky bit must be set on all SUSE operating system world-writable directories.

```
GROUP ID: V-234828
RULE ID: SV-234828r958524
```

Rationale:

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

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

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

Audit:

Verify the SUSE operating system prevents unauthorized and unintended information transfer via the shared system resources.

Check that world-writable directories have the sticky bit set with the following command:

```
sudo find / \( -path /.snapshots -o -path /sys -o -path /proc \) -prune -o -
perm -002 -type d -exec ls -lLd {} \;

256 0 drwxrwxrwt 1 root root 4096 Jun 14 06:45 /tmp
```

If any of the returned directories do not have the sticky bit set, or are not documented as having the write permission for the other class, this is a finding.

Remediation:

Configure the SUSE operating system shared system resources to prevent any unauthorized and unintended information transfer by setting the sticky bit for all world-writable directories.

An example of a world-writable directory is "/tmp" directory. Set the sticky bit on all of the world-writable directories (using the "/tmp" directory as an example) with the following command:

```
sudo chmod 1777 /tmp
```

For every world-writable directory, replace "/tmp" in the command above with the world-writable directory that does not have the sticky bit set.

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

1.28 SLES-15-010310 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must be configured to use TCP syncookies.

```
GROUP ID: V-234829
RULE ID: SV-234829r958528
```

Rationale:

Denial of Service (DoS) is a condition in which a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

Managing excess capacity ensures that sufficient capacity is available to counter flooding attacks. Employing increased capacity and service redundancy may reduce the susceptibility to some DoS attacks. Managing excess capacity may include, for example, establishing selected usage priorities, quotas, or partitioning.

Audit:

Verify the SUSE operating system is configured to use IPv4 TCP syncookies.

Check to see if syncookies are used with the following command:

```
sudo sysctl net.ipv4.tcp_syncookies
net.ipv4.tcp_syncookies = 1
```

If the network parameter "ipv4.tcp_syncookies" is not equal to "1" or nothing is returned, this is a finding.

Remediation:

Configure the SUSE operating system to use IPv4 TCP syncookies by running the following command as an administrator:

```
sudo sysctl -w net.ipv4.tcp_syncookies=1
```

If "1" is not the system's default value, add or update the following line in "/etc/sysctl.d/99-stig.conf":

```
sudo sh -c 'echo "net.ipv4.tcp_syncookies=1" >> /etc/sysctl.d/99-stig.conf'
sudo sysctl --system
```

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

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

1.29 SLES-15-010320 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system for all network connections associated with SSH traffic must immediately terminate at the end of the session or after 10 minutes of inactivity.

```
GROUP ID: V-234830
RULE ID: SV-234830r1069400
```

Rationale:

Automatic session termination addresses the termination of user-initiated logical sessions in contrast to the termination of network connections associated with communications sessions (i.e., network disconnect). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational information system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions.

Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated.

Conditions or trigger events requiring automatic session termination can include, for example, organization-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on information system use.

This capability is typically reserved for specific SUSE operating system functionality where the system owner, data owner, or organization requires additional assurance.

In Linux, ClientAliveCountMax directive is used in the SSH daemon configuration file to define the number of client alive messages the SSH server will send without receiving any response from the client before terminating the session. The ClientAliveInterval (SLES-15-010280/ V-234827) sets a timeout interval in seconds after which if no data has been received from the client, the ssh daemon will send a message through the encrypted channel to request a response from the client. Together, these two settings provide a way to configure a timeout for inactive sessions.

Audit:

Verify that all network connections associated with SSH traffic are automatically terminated at the end of the session or after 10 minutes of inactivity.

Check that the "ClientAliveCountMax" variable is set to a value of "1" or less by performing the following command:

```
sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' | tr
'\n' ' ' | xargs sudo grep -iH '^\s*clientalivecountmax'

ClientAliveCountMax 1
```

If "ClientAliveCountMax" does not exist or "ClientAliveCountMax" is not set to a value of "1" in "/etc/ssh/sshd_config", or the line is commented out, this is a finding.

Remediation:

Configure the SUSE operating system to automatically terminate all network connections associated with SSH traffic at the end of a session or after a 10-minute period of inactivity.

Modify or append the following lines in the "/etc/ssh/sshd_config" file:

```
ClientAliveCountMax 1
```

For the changes to take effect, the SSH daemon must be restarted.

```
sudo systemctl restart sshd.service
```

Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::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

1.30 SLES-15-010330 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

All SUSE operating system persistent disk partitions must implement cryptographic mechanisms to prevent unauthorized disclosure or modification of all information that requires at-rest protection.

```
GROUP ID: V-234831
RULE ID: SV-234831r1009558
```

Rationale:

SUSE operating systems handling data requiring data-at-rest protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest.

Selection of a cryptographic mechanism is based on the need to protect the integrity of organizational information. The strength of the mechanism is commensurate with the security category and/or classification of the information. Organizations have the flexibility to either encrypt all information on storage devices (i.e., full disk encryption) or encrypt specific data structures (e.g., files, records, or fields).

Satisfies: SRG-OS-000185-GPOS-00079, SRG-OS-000404-GPOS-00183, SRG-OS-000405-GPOS-00184

Audit:

Verify the SUSE operating system prevents unauthorized disclosure or modification of all information requiring at rest protection by using disk encryption.

Determine the partition layout for the system with the following command:

```
sudo fdisk -l

Device Boot Start End Sectors Size Id Type
/dev/sda1 2048 4208639 4206592 2G 82 Linux swap
/dev/sda2 * 4208640 53479423 49270784 23.5G 83 Linux
/dev/sda3 53479424 125829119 72349696 34.5G 83 Linux
```

Verify the system partitions are all encrypted with the following command:

```
sudo more /etc/crypttab

cr_root  UUID=26d4a101-7f48-4394-b730-56dc00e65f64
cr_home  UUID=f5b8a790-14cb-4b82-882d-707d52f27765
cr_swap  UUID=f2d86128-f975-478d-a5b0-25806c900eac
```

Every persistent disk partition present on the system must have an entry in the file.

If any partitions other than pseudo file systems (such as /proc or /sys) are not listed or "/etc/crypttab" does not exist, this is a finding.

Remediation:

Configure the SUSE operating system to prevent unauthorized modification of all information at rest by using disk encryption.

Encrypting a partition in an already-installed system is more difficult because of the need to resize and change existing partitions. To encrypt an entire partition, dedicate a partition for encryption in the partition layout. The standard partitioning proposal as suggested by YaST (installation and configuration tool for Linux) does not include an encrypted partition by default. Add it manually in the partitioning dialog.

Refer to the document "SUSE Linux Enterprise Server 15 SP1 - Security Guide", Section 12.1.2, for a detailed disk encryption guide:

https://documentation.suse.com/sles/15-SP1/html/SLES-all/cha-security-cryptofs.html#sec-security-cryptofs-y2-part-run

Additional Information:

CCI-001199 Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

CCI-002475 Implement cryptographic mechanisms to prevent unauthorized modification 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)

1.31 SLES-15-010340 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.

```
GROUP ID: V-234832
RULE ID: SV-234832r958564
```

Rationale:

Any operating system providing too much information in error messages risks compromising the data and security of the structure, and content of error messages needs to be carefully considered by the organization.

Organizations carefully consider the structure/content of error messages. The extent to which information systems are able to identify and handle error conditions is guided by organizational policy and operational requirements. Information that could be exploited by adversaries includes, for example, erroneous logon attempts with passwords entered by mistake as the username, mission/business information that can be derived from (if not stated explicitly by) information recorded, and personal information, such as account numbers, social security numbers, and credit card numbers.

The /var/log/btmp, /var/log/wtmp, and /var/log/lastlog files have group write and global read permissions to allow for the lastlog function to perform. Limiting the permissions beyond this configuration will result in the failure of functions that rely on the lastlog database.

Audit:

Verify the SUSE operating system has all system log files under the /var/log directory with a permission set to "640", by using the following command:

Note: The btmp, wtmp, and lastlog files are excluded. Refer to the Discussion for details.

```
sudo find /var/log -perm /137 ! -name '*[bw]tmp' ! -name '*lastlog' -type f -
exec stat -c "%n %a" {} \;
```

If command displays any output, this is a finding.

Remediation:

Configure the SUSE operating system to set permissions of all log files under /var/log directory to "640" or more restricted, by using the following command:

Note: The btmp, wtmp, and lastlog files are excluded. Refer to the Discussion for details.

```
sudo find /var/log -perm /137 ! -name '*[bw]tmp' ! -name '*lastlog' -type f -
exec chmod 640 '{}' \;
```

Additional Information:

CCI-001312 Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

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

1.32 SLES-15-010350 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must prevent unauthorized users from accessing system error messages.

```
GROUP ID: V-234833
RULE ID: SV-234833r958566
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the SUSE operating system or platform. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

Verify the SUSE operating system prevents unauthorized users from accessing system error messages.

Check the "/var/log/messages" file permissions with the following command:

```
sudo stat -c "%n %U:%G %a" /var/log/messages

/var/log/messages root:root 640
```

Check that "permissions.local" file contains the correct permissions rules with the following command:

```
grep -i messages /etc/permissions.local

/var/log/messages root:root 640
```

If the effective permissions do not match the "permissions.local" file, the command does not return any output, or is commented out, this is a finding.

Remediation:

Configure the SUSE operating system to prevent unauthorized users from accessing system error messages.

Add or update the following rules in "/etc/permissions.local":

```
/var/log/messages root:root 640
```

Set the correct permissions with the following command:

```
sudo chkstat --set --system
```

Additional Information:

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

1.33 SLES-15-010351 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system library files must have mode 0755 or less permissive.

```
GROUP ID: V-234834
RULE ID: SV-234834r991560
```

Rationale:

If the SUSE operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to SUSE operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system-wide shared library files contained in the directories "/lib", "/lib64", "/usr/lib", and "/usr/lib64" have mode "0755" or less permissive.

Check that the system-wide shared library files have mode "0755" or less permissive with the following command:

```
sudo find /lib /lib64 /usr/lib /usr/lib64 -perm /022 -type f -exec stat -c
"%n %a" '{}' \;
```

If any files are found to be group-writable or world-writable, this is a finding.

Remediation:

Configure the library files to be protected from unauthorized access. Run the following command:

```
sudo find /lib /lib64 /usr/lib /usr/lib64 -perm /022 -type f -exec chmod 755
'{}' \;
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

1.34 SLES-15-010352 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system library directories must have mode 0755 or less permissive.

```
GROUP ID: V-234835
RULE ID: SV-234835r991560
```

Rationale:

If the SUSE operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to SUSE operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system-wide shared library directories "/lib", "/lib64", "/usr/lib" and "/usr/lib64" have mode "0755" or less permissive.

Check that the system-wide shared library directories have mode "0755" or less permissive with the following command:

```
sudo find /lib /lib64 /usr/lib /usr/lib64 -perm /022 -type d -exec stat -c
"%n %a" '{}' \;
```

If any of the aforementioned directories are found to be group-writable or world-writable, this is a finding.

Remediation:

Configure the shared library directories to be protected from unauthorized access. Run the following command:

```
sudo find /lib /lib64 /usr/lib /usr/lib64 -perm /022 -type d -exec chmod 755
'{}' \;
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

1.35 SLES-15-010353 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system library files must be owned by root.

```
GROUP ID: V-234836
RULE ID: SV-234836r991560
```

Rationale:

If the SUSE operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to SUSE operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system-wide shared library files contained in the directories "/lib", "/lib64", "/usr/lib" and "/usr/lib64" are owned by root.

Check that the system-wide shared library files are owned by root with the following command:

```
sudo find /lib /lib64 /usr/lib /usr/lib64 ! -user root -type f -exec stat -c
"%n %U" '{}' \;
```

If any system wide library file is returned, this is a finding.

Remediation:

Configure the system library files to be protected from unauthorized access. Run the following command:

```
sudo find /lib /lib64 /usr/lib /usr/lib64 ! -user root -type f -exec chown
root '{}' \;
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

1.36 SLES-15-010354 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system library directories must be owned by root.

```
GROUP ID: V-234837
RULE ID: SV-234837r991560
```

Rationale:

If the SUSE operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to SUSE operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system-wide shared library directories "/lib", "/lib64", "/usr/lib/" and "/usr/lib64" are owned by root.

Check that the system-wide shared library directories are owned by root with the following command:

```
sudo find /lib /lib64 /usr/lib /usr/lib64 ! -user root -type d -exec stat -c
"%n %U" '{}' \;
```

If any system wide library directory is returned, this is a finding.

Remediation:

Configure the library files and their respective parent directories to be protected from unauthorized access. Run the following command:

```
sudo find /lib /lib64 /usr/lib /usr/lib64 ! -user root -type d -exec chown
root '{}' \;
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

1.37 SLES-15-010355 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system library files must be group-owned by root.

```
GROUP ID: V-234838
RULE ID: SV-234838r991560
```

Rationale:

If the SUSE operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to SUSE operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system-wide library files contained in the directories "/lib", "/lib64", "/usr/lib" and "/usr/lib64" are group-owned by root.

Check that the system-wide library files are group-owned by root with the following command:

```
sudo find /lib /lib64 /usr/lib /usr/lib64 ! -group root -type f -exec stat -c
"%n %G" '{}' \;
```

If any system wide shared library file is returned, this is a finding.

Remediation:

Configure the system library files to be protected from unauthorized access. Run the following command:

```
sudo find /lib /lib64 /usr/lib /usr/lib64 ! -group root -type f -exec chgrp
root '{}' \;
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

1.38 SLES-15-010356 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system library directories must be group-owned by root.

```
GROUP ID: V-234839
RULE ID: SV-234839r991560
```

Rationale:

If the SUSE operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to SUSE operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system-wide library directories "/lib", "/lib64", "/usr/lib" and "/usr/lib64" are group-owned by root.

Check that the system-wide library directories are group-owned by root with the following command:

```
sudo find /lib /lib64 /usr/lib /usr/lib64 ! -group root -type d -exec stat -c
"%n %G" '{}' \;
```

If any system wide shared library directory is returned, this is a finding.

Remediation:

Configure the system library directories to be protected from unauthorized access. Run the following command:

```
sudo find /lib /lib64 /usr/lib /usr/lib64 ! -group root -type d -exec chgrp
root '{}' \;
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

1.39 SLES-15-010357 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must have system commands set to a mode of 0755 or less permissive.

```
GROUP ID: V-234840
RULE ID: SV-234840r991560
```

Rationale:

If the SUSE operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to SUSE operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system commands contained in the following directories have mode "0755" or less permissive:

```
/bin
/sbin
/usr/bin
/usr/sbin
/usr/local/bin
/usr/local/sbin
```

Check that the system command files have mode "0755" or less permissive with the following command:

```
find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin -perm
/022 -type f -exec stat -c "%n %a" '{}' \;
```

If any files are found to be group-writable or world-writable, this is a finding.

Remediation:

Configure the system commands to be protected from unauthorized access. Run the following command:

```
sudo find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin -
perm /022 -type f -exec chmod 755 '{}' \;
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

1.40 SLES-15-010358 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must have directories that contain system commands set to a mode of 0755 or less permissive.

```
GROUP ID: V-234841
RULE ID: SV-234841r991560
```

Rationale:

If the SUSE operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to SUSE operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system commands directories have mode "0755" or less permissive:

```
/bin
/sbin
/usr/bin
/usr/sbin
/usr/local/bin
/usr/local/sbin
```

Check that the system command directories have mode "0755" or less permissive with the following command:

```
find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin -perm
/022 -type d -exec stat -c "%n %a" '{}' \;
```

If any directories are found to be group-writable or world-writable, this is a finding.

Remediation:

Configure the system commands directories to be protected from unauthorized access. Run the following command:

```
sudo find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin -
perm /022 -type d -exec chmod -R 755 '{}' \;
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

1.41 SLES-15-010359 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must have system commands owned by root.

```
GROUP ID: V-234842
RULE ID: SV-234842r991560
```

Rationale:

If the SUSE operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to SUSE operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system commands contained in the following directories are owned by root:

```
/bin
/sbin
/usr/bin
/usr/sbin
/usr/local/bin
/usr/local/sbin
```

Use the following command for the check:

```
sudo find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -
user root -type f -exec stat -c "%n %U" '{}' \;
```

If any system commands are returned, this is a finding.

Remediation:

Configure the system commands - and their respective parent directories - to be protected from unauthorized access. Run the following command:

```
sudo find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -
user root -type f -exec chown root '{}' \;
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

1.42 SLES-15-010360 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must have directories that contain system commands owned by root.

```
GROUP ID: V-234843
RULE ID: SV-234843r991560
```

Rationale:

If the SUSE operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to SUSE operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system commands directories are owned by root:

```
/bin
/sbin
/usr/bin
/usr/sbin
/usr/local/bin
/usr/local/sbin
```

Use the following command for the check:

```
sudo find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -
user root -type d -exec stat -c "%n %U" '{}' \;
```

If any system commands directories are returned, this is a finding.

Remediation:

Configure the system commands directories to be protected from unauthorized access. Run the following command:

```
sudo find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -
user root -type d -exec chown root '{}' \;
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

1.43 SLES-15-010361 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must have system commands group-owned by root or a system account.

```
GROUP ID: V-234844
RULE ID: SV-234844r991560
```

Rationale:

If the SUSE operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to SUSE operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system commands contained in the following directories are group-owned by root or a system account:

```
/bin
/sbin
/usr/bin
/usr/sbin
/usr/local/bin
/usr/local/sbin
```

Run the check with the following command:

```
sudo find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -
group root -type f -exec stat -c "%n %G" '{}' \;
```

If any system commands are returned that are not Set Group ID upon execution (SGID) files and group-owned by a required system account, this is a finding.

Remediation:

Configure the system commands to be protected from unauthorized access. Run the following command, replacing "[FILE]" with any system command file not group-owned by "root" or a required system account.

```
sudo chgrp root [FILE]
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

1.44 SLES-15-010362 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must have directories that contain system commands group-owned by root.

```
GROUP ID: V-234845
RULE ID: SV-234845r991560
```

Rationale:

If the SUSE operating system were to allow any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to SUSE operating systems with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs which execute with escalated privileges. Only qualified and authorized individuals must be allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications.

Audit:

Verify the system commands directories are group-owned by root:

```
/bin
/sbin
/usr/bin
/usr/sbin
/usr/local/bin
/usr/local/sbin
```

Run the check with the following command:

```
sudo find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -
group root -type d -exec stat -c "%n %G" '{}' \;
```

If any system commands directories are returned that are not Set Group ID up on execution (SGID) files and owned by a privileged account, this is a finding.

Remediation:

Configure the system commands directories to be protected from unauthorized access. Run the following command:

```
sudo find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -
group root -type d -exec chgrp root '{}' \;
```

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

- NIST SP 800-53::CM-5 (6)
- NIST SP 800-53A::CM-5 (6).1
- NIST SP 800-53 Revision 4::CM-5 (6)
- NIST SP 800-53 Revision 5::CM-5 (6)

1.45 SLES-15-010370 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must have a firewall system installed to immediately disconnect or disable remote access to the whole operating system.

```
GROUP ID: V-234846
RULE ID: SV-234846r958674
```

Rationale:

Operating system remote access functionality must have the capability to immediately disconnect current users remotely accessing the information system and/or disable further remote access. The speed of disconnect or disablement varies based on the criticality of mission functions and the need to eliminate immediate or future remote access to organizational information systems.

SUSE operating systems are capable to immediately stop remote connections and services by a local system administrator.

To immediately disconnect or disable remote access, the firewall needs to be set into panic mode.

```
sudo firewall-cmd --panic-on
```

To enable remote connection again, panic mode needs to be disabled.

```
sudo firewall-cmd --panic-off
```

Audit:

Verify "firewalld" is configured to protect the SUSE operating system.

Run the following command:

```
systemctl status firewalld.service
 firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor
preset: disabled)
   Active: active (running) since Wed 2019-11-06 10:58:11 CET; 24h ago
     Docs: man:firewalld(1)
 Main PID: 1105 (firewalld)
    Tasks: 2 (limit: 4915)
   CGroup: /system.slice/firewalld.service
           ??1105 /usr/bin/python3 -Es /usr/sbin/firewalld --nofork --nopid
```

If the service is not enabled, this is a finding.

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

Remediation:

Configure the SUSE operating system to enable the firewall service. This is needed to be able to immediately disconnect or disable remote access to the whole system.

Enable the "firewalld.service" by running the following command:

```
sudo systemctl enable firewalld.service
```

Start the "firewalld.service" by running the following command:

```
sudo systemctl start firewalld.service
```

To immediately disconnect or disable remote access the firewall needs to be set into panic mode.

```
sudo firewall-cmd --panic-on
```

To enable remote connection again, panic mode needs to be disabled.

```
sudo firewall-cmd --panic-off
```

Additional Information:

CCI-002322 Provide the capability to disconnect or disable remote access to the system within the organization-defined time period.

- NIST SP 800-53 Revision 4::AC-17 (9)
- NIST SP 800-53 Revision 5::AC-17 (9)

1.46 SLES-15-010375 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

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

```
GROUP ID: V-255921
RULE ID: SV-255921r958524
```

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

1.47 SLES-15-010380 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system wireless network adapters must be disabled unless approved and documented.

```
GROUP ID: V-234847
RULE ID: SV-234847r991568
```

Rationale:

Without protection of communications with wireless peripherals, confidentiality and integrity may be compromised because unprotected communications can be intercepted and either read, altered, or used to compromise the SUSE operating system.

This requirement applies to wireless peripheral technologies (e.g., wireless mice, keyboards, displays, etc.) used with a SUSE operating system. Wireless peripherals (e.g., Wi-Fi/Bluetooth/IR Keyboards, Mice, and Pointing Devices and Near Field Communications [NFC]) present a unique challenge by creating an open, unsecured port on a computer. Wireless peripherals must meet DoD requirements for wireless data transmission and be approved for use by the AO. Even though some wireless peripherals, such as mice and pointing devices, do not ordinarily carry information that need to be protected, modification of communications with these wireless peripherals may be used to compromise the SUSE operating system. Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification.

Protecting the confidentiality and integrity of communications with wireless peripherals can be accomplished by physical means (e.g., employing physical barriers to wireless radio frequencies) or by logical means (e.g., employing cryptographic techniques). If physical means of protection are employed, then logical means (cryptography) do not have to be employed, and vice versa. If the wireless peripheral is only passing telemetry data, encryption of the data may not be required.

Satisfies: SRG-OS-000299-GPOS-00117, SRG-OS-000300-GPOS-00118, SRG-OS-000481-GPOS-000481

Audit:

Verify that the SUSE operating system has no wireless network adapters enabled.

Check that there are no wireless interfaces configured on the system with the following command:

```
sudo wicked show all

lo up
link: #1, state up
type: loopback
config: compat:suse:/etc/sysconfig/network/ifcfg-lo
leases: ipv4 static granted
leases: ipv6 static granted
addr: ipv4 127.0.0.1/8 [static]
addr: ipv6 ::1/128 [static]

eth0 up
link: #2, state up, mtu 1500
type: ethernet, hwaddr 06:00:00:00:00:01
config: compat:suse:/etc/sysconfig/network/ifcfg-eth0
leases: ipv4 dhcp granted
leases: ipv6 dhcp granted, ipv6 auto granted
addr: ipv4 10.0.0.100/16 [dhcp]
route: ipv4 default via 10.0.0.1 proto dhcp

wlan0 up
link: #3, state up, mtu 1500
type: wireless, hwaddr 06:00:00:00:00:02
config: wicked:xml:/etc/wicked/ifconfig/wlan0.xml
leases: ipv4 dhcp granted
addr: ipv4 10.0.0.101/16 [dhcp]
route: ipv4 default via 10.0.0.1 proto dhcp
```

If a wireless interface is configured, it must be documented and approved by the local AO.

If a wireless interface is configured and has not been documented and approved, this is a finding.

Remediation:

Configure the SUSE operating system to disable all wireless network interfaces with the following command:

For each interface of type wireless, bring the interface into "down" state:

```
sudo wicked ifdown wlan0
```

For each interface of type wireless with a configuration type of "compat:suse:", remove the associated file:

```
sudo rm /etc/sysconfig/network/ifcfg-wlan0
```

For each interface of type wireless, for each configuration of type "wicked:xml:", remove the associated file or remove the interface configuration from the file.

```
sudo rm /etc/wicked/ifconfig/wlan0.xml
```

Additional Information:

CCI-001443 Protect wireless access to the system using authentication of users and/or devices.

- NIST SP 800-53::AC-18 (1)
- NIST SP 800-53A::AC-18 (1).1
- NIST SP 800-53 Revision 4::AC-18 (1)
- NIST SP 800-53 Revision 5::AC-18 (1)

CCI-001444 Protect wireless access to the system using encryption.

- NIST SP 800-53::AC-18 (1)
- NIST SP 800-53A::AC-18 (1).1
- NIST SP 800-53 Revision 4::AC-18 (1)
- NIST SP 800-53 Revision 5::AC-18 (1)

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4::SC-8
- NIST SP 800-53 Revision 5::SC-8

1.48 SLES-15-010390 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

SUSE operating system AppArmor tool must be configured to control whitelisted applications and user home directory access control.

```
GROUP ID: V-234848
RULE ID: SV-234848r958702
```

Rationale:

Using a whitelist provides a configuration management method for allowing the execution of only authorized software. Using only authorized software decreases risk by limiting the number of potential vulnerabilities.

The organization must identify authorized software programs and permit execution of authorized software by adding each authorized program to the "pam_apparmor" exception policy. The process used to identify software programs that are authorized to execute on organizational information systems is commonly referred to as whitelisting.

Verification of whitelisted software occurs prior to execution or at system startup.

Users' home directories/folders may contain information of a sensitive nature. Nonprivileged users should coordinate any sharing of information with a System Administrator (SA) through shared resources.

AppArmor can confine users to their home directory, not allowing them to make any changes outside of their own home directories. Confining users to their home directory will minimize the risk of sharing information.

Satisfies: SRG-OS-000312-GPOS-00122, SRG-OS-000312-GPOS-00123, SRG-OS-000312-GPOS-00124, SRG-OS-000324-GPOS-00125, SRG-OS-000326-GPOS-00126, SRG-OS-000368-GPOS-00154, SRG-OS-000370-GPOS-00155, SRG-OS-000480-GPOS-00230

Audit:

Verify that the SUSE operating system AppArmor tool is configured to control whitelisted applications and user home directory access control.

Check that "pam_apparmor" is installed on the system with the following command:

```
zypper info pam_apparmor | grep "Installed"
```

If the package "pam_apparmor" is not installed on the system, this is a finding.

Check that the "apparmor" daemon is running with the following command:

```
systemctl status apparmor.service | grep -i active

Active: active (exited) since Fri 2017-01-13 01:01:01 GMT; 1day 1h ago
```

If something other than "Active: active" is returned, this is a finding.

Note: "pam_apparmor" must have properly configured profiles. All configurations will be based on the actual system setup and organization. See the "pam_apparmor" documentation for more information on configuring profiles.

Remediation:

Configure the SUSE operating system to blacklist all applications by default and permit by whitelist.

Install "pam_apparmor" (if it is not installed) with the following command:

```
sudo zypper in pam_apparmor
```

Enable/activate "Apparmor" (if it is not already active) with the following command:

```
sudo systemctl enable apparmor.service
```

Start "Apparmor" with the following command:

```
sudo systemctl start apparmor.service
```

Note: "pam_apparmor" must have properly configured profiles. All configurations will be based on the actual system setup and organization. See the "pam_apparmor" documentation for more information on configuring profiles.

Additional Information:

CCI-001764 Prevent program execution in accordance with organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

- NIST SP 800-53 Revision 4::CM-7 (2)
- NIST SP 800-53 Revision 5::CM-7 (2)

CCI-001774 Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system.

- NIST SP 800-53 Revision 4::CM-7 (5) (b)
- NIST SP 800-53 Revision 5::CM-7 (5) (b)

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-002233 Prevent the organization-defined software from executing at higher privilege levels than users executing the software.

- NIST SP 800-53 Revision 4::AC-6 (8)
- NIST SP 800-53 Revision 5::AC-6 (8)

CCI-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)

1.49 SLES-15-010400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system clock must, for networked systems, be synchronized to an authoritative DOD time source at least every 24 hours.

```
GROUP ID: V-234849
RULE ID: SV-234849r1038944
```

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:

The SUSE operating system clock must be configured to synchronize to an authoritative DOD time source when the time difference is greater than one second.

Check that the SUSE operating system clock must be configured to synchronize to an authoritative DOD time source when the time difference is greater than one second with the following command:

```
sudo grep maxpoll /etc/chrony.conf

server 0.us.pool.ntp.mil maxpoll 16
```

If nothing is returned, "maxpoll" is greater than "16", or is commented out, this is a finding.

Verify the "chrony.conf" file is configured to an authoritative DOD time source by running the following command:

```
sudo grep -i server /etc/chrony.conf
server 0.us.pool.ntp.mil
```

If the parameter "server" is not set, is not set to an authoritative DOD time source, or is commented out, this is a finding.

Remediation:

The SUSE operating system clock must be configured to synchronize to an authoritative DOD time source when the time difference is greater than one second.

To configure the system clock to synchronize to an authoritative DOD time source at least every 24 hours, edit the file "/etc/chrony.conf". Add or correct the following lines by replacing "[time_source]" with an authoritative DOD time source:

```
server [time_source] maxpoll 16
```

Additional Information:
CCI-004923 Compare the internal system clocks on an organization-defined frequency with organization-defined authoritative time source.

- NIST SP 800-53 Revision 5::SC-45 (1) (a)

CCI-004926 Synchronize the internal system clocks to the authoritative time source when the time difference is greater than organization-defined time period.

- NIST SP 800-53 Revision 5::SC-45 (1) (b)

CCI-001891 The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source.

- NIST SP 800-53 Revision 4::AU-8 (1) (a)

CCI-002046 The information system synchronizes the internal system clocks to the authoritative time source when the time difference is greater than the organization-defined time period.

- NIST SP 800-53 Revision 4::AU-8 (1) (b)

1.50 SLES-15-010410 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The SUSE operating system must be configured to use Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).

```
GROUP ID: V-234850
RULE ID: SV-234850r958788
```

Rationale:

If time stamps are not consistently applied and there is no common time reference, it is difficult to perform forensic analysis.

Time stamps generated by the SUSE operating system include date and time. Time is commonly expressed in UTC, a modern continuation of GMT, or local time with an offset from UTC.

Audit:

Verify the SUSE operating system is configured to use UTC or GMT.

Check that the SUSE operating system is configured to use UTC or GMT with the following command:

```
timedatectl status | grep -i "time zone"
Time zone: UTC (UTC, +0000)
```

If "Time zone" is not set to "UTC" or "GMT", this is a finding.

Remediation:

Configure the SUSE operating system is configured to use UTC or GMT.

To configure the system time zone to use UTC or GMT, run the following command, replacing [ZONE] with "UTC" or "GMT".

```
sudo timedatectl set-timezone [ZONE]
```

Additional Information:

CCI-001890 Record time stamps for audit records that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

- NIST SP 800-53 Revision 4::AU-8 b
- NIST SP 800-53 Revision 5::AU-8 b

1.51 SLES-15-010418 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must be configured to allow sending email notifications of unauthorized configuration changes to designated personnel.

```
GROUP ID: V-256983
RULE ID: SV-256983r958794
```

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 zypper se mailx

i | mailx | A MIME-Capable Implementation of the mailx Command | package
```

If "mailx" package is not installed, this is a finding.

Remediation:

Install the "mailx" package on the system:

```
sudo zypper 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)

1.52 SLES-15-010419 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must use a file integrity tool to verify correct operation of all security functions.

```
GROUP ID: V-255922
RULE ID: SV-255922r958794
```

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 SUSE 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 zypper if aide | grep "Installed"
Installed: Yes
```

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 aide --check
```

If the output is "Couldn't open file /var/lib/aide/aide.db for reading", this is a finding.

Remediation:

Install AIDE, initialize it, and perform a manual check.

Install AIDE:

```
$ sudo zipper in aide
```

Initialize it (this may take a few minutes):

```
$ sudo aide -i
```

The new database will need to be renamed to be read by AIDE:

```
$ sudo mv /var/lib/aide/aide.db.new /var/lib/aide/aide.db
```

Perform a manual check:``

```
$ sudo aide --check
```

Example output:

```
 Summary:
       Total number of files:        140621
       Added files:                  1
       Removed files:                1
       Changed files:                0

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

1.53 SLES-15-010420 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Advanced Intrusion Detection Environment (AIDE) must verify the baseline SUSE operating system configuration at least weekly.

```
GROUP ID: V-234851
RULE ID: SV-234851r958794
```

Rationale:

Unauthorized changes to the baseline configuration could make the system vulnerable to various attacks or allow unauthorized access to the SUSE operating system. Changes to SUSE 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 SUSE operating system. The SUSE operating system's Information System Security Manager (ISSM)/Information System Security Officer (ISSO) and System Administrator (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, SRG-OS-000445-GPOS-00199, SRG-OS-000446-GPOS-00200

Audit:

Verify the SUSE operating system checks the baseline configuration for unauthorized changes at least once weekly.

Note: A file integrity tool other than 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 to scan for changes to the system baseline. The command used in the following example looks at the daily cron job:

Check the "/etc/cron" subdirectories for a "crontab" file controlling the execution of the file integrity application. For example, if AIDE is installed on the system, use the following command:

```
sudo grep -R aide /etc/crontab /etc/cron.*

/etc/crontab: 30 04 * * * /etc/aide
```

If the file integrity application does not exist, or a "crontab" file does not exist in "/etc/crontab", the "/etc/cron.daily" subdirectory, or "/etc/cron.weekly" subdirectory, this is a finding.

Remediation:

Configure the SUSE operating system to check the baseline configuration for unauthorized changes at least once weekly.

If the "aide" package is not installed, install it with the following command:

```
sudo zypper in aide
```

Configure the file integrity tool to automatically run on the system at least weekly. The following example output is generic. It will set cron to run AIDE weekly, but other file integrity tools may be used:

```
cat /etc/cron.weekly/aide

0 0 * * * /usr/sbin/aide --check | /bin/mail -s "$HOSTNAME - Daily AIDE
integrity check run" root@example_server_name.mil
```

Note: Per requirement SLES-15-010418, 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-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

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

1.54 SLES-15-010430 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The SUSE operating system tool zypper must have gpgcheck enabled.

```
GROUP ID: V-234852
RULE ID: SV-234852r1009613
```

Rationale:

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

Accordingly, patches, service packs, device drivers, or SUSE 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 ensures 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 SUSE 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 Certification Authority (CA).

Audit:

Verify that the SUSE operating system tool zypper has gpgcheck enabled.

Check that zypper has gpgcheck enabled with the following command:

```
grep -i '^gpgcheck' /etc/zypp/zypp.conf

gpgcheck = 1
```

If "gpgcheck" is set to "0", "off", "no", or "false", this is a finding.

Remediation:

Configure that the SUSE operating system tool zypper to enable gpgcheck by editing or adding the following line to "/etc/zypp/zypp.conf":

```
gpgcheck = 1
```

Additional Information:

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

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

CCI-001749 The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

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

1.55 SLES-15-010450 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The SUSE operating system must reauthenticate users when changing authenticators, roles, or escalating privileges.

```
GROUP ID: V-234853
RULE ID: SV-234853r1050789
```

Rationale:

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

When the SUSE operating system provides the capability to change user authenticators, change security roles, or 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 that the SUSE operating system requires reauthentication when changing authenticators, roles, or escalating privileges.

Check that "/etc/sudoers" has no occurrences of "NOPASSWD" or "!authenticate" with the following command:

```
sudo egrep -i '(nopasswd|!authenticate)' /etc/sudoers
```

If any uncommented lines containing "!authenticate", or "NOPASSWD" are returned and active accounts on the system have valid passwords, this is a finding.

Remediation:

Configure the SUSE operating system to remove any occurrence of "NOPASSWD" or "!authenticate" found in the "/etc/sudoers" file. If the system does not use passwords for authentication, the "NOPASSWD" tag may exist in the file.

Additional Information:

CCI-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5::SC-11 b

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

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

1.56 SLES-15-010460 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must have the packages required for multifactor authentication to be installed.

```
GROUP ID: V-234854
RULE ID: SV-234854r1009615
```

Rationale:

Using an authentication device, such as a Common Access Card (CAC) or token 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 (PIV) card and the DOD CAC.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-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-000376-GPOS-00161, SRG-OS-000377-GPOS-00162

Audit:

Verify the SUSE 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:

```
zypper info pam_pkcs11 | grep -i installed
zypper info mozilla-nss | grep -i installed
zypper info mozilla-nss-tools | grep -i installed
zypper info pcsc-ccid | grep -i installed
zypper info pcsc-lite | grep -i installed
zypper info pcsc-tools | grep -i installed
zypper info opensc | grep -i installed
zypper info coolkey | grep -i installed
```

If any of the packages required for multifactor authentication are not installed, this is a finding.

Remediation:

Configure the SUSE operating system to implement multifactor authentication by installing the required packages.

Install the packages required to support multifactor authentication with the following commands:

```
zypper install pam_pkcs11
zypper install mozilla-nss
zypper install mozilla-nss-tools
zypper install pcsc-ccid
zypper install pcsc-lite
zypper install pcsc-tools
zypper install opensc
zypper install coolkey
```

Additional information on the configuration of multifactor authentication on the SUSE operating system can be found at https://www.suse.com/communities/blog/configuring-smart-card-authentication-suse-linux-enterprise/.

Additional Information:

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

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

CCI-001953 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)

CCI-001948 The information system implements multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

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

1.57 SLES-15-010470 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must implement certificate status checking for multifactor authentication.

```
GROUP ID: V-234855
RULE ID: SV-234855r1009616
```

Rationale:

Using an authentication device, such as a Common Access Card (CAC) or token separate from the information system, ensures credentials stored on the authentication device will not be affected if the information system is compromised.

Multifactor solutions that require devices separate from information systems to gain access include hardware tokens providing time-based or challenge-response authenticators, and smart cards such as the U.S. Government Personal Identity Verification (PIV) card and the DOD CAC.

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, non-organization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

This requirement only applies to components with device-specific functions, or for organizational users (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-000376-GPOS-00161, SRG-OS-000377-GPOS-00162

Audit:

Verify the SUSE operating system implements certificate status checking for multifactor authentication.

Check that certificate status checking for multifactor authentication is implemented with the following command:

```
grep use_pkcs11_module /etc/pam_pkcs11/pam_pkcs11.conf | awk '/pkcs11_module
coolkey {/,/}/' /etc/pam_pkcs11/pam_pkcs11.conf | grep cert_policy

cert_policy = ca,ocsp_on,signature,crl_auto;
```

If "cert_policy" is not set to include "ocsp", this is a finding.

Remediation:

Configure the SUSE operating system to certificate status checking for PKI authentication.

Modify all of the cert_policy lines in "/etc/pam_pkcs11/pam_pkcs11.conf" to include "ocsp_on".

Note: OCSP allows sending request for certificate status information. Additional certificate validation polices are permitted.

Additional information on the configuration of multifactor authentication on the SUSE operating system can be found at https://www.suse.com/communities/blog/configuring-smart-card-authentication-suse-linux-enterprise/.

Additional Information:

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

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

CCI-001953 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)

CCI-001948 The information system implements multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

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

1.58 SLES-15-010480 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must disable the USB mass storage kernel module.

```
GROUP ID: V-234856
RULE ID: SV-234856r958820
```

Rationale:

Without identifying devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity.

Peripherals include but are not limited to such devices as flash drives, external storage, and printers.

Audit:

Verify the SUSE operating system does not automount USB mass storage devices when connected to the host.

Check that "usb-storage" is blacklisted in the "/etc/modprobe.d/50-blacklist.conf" file with the following command:

```
grep usb-storage /etc/modprobe.d/50-blacklist.conf

blacklist usb-storage
```

If nothing is output from the command, this is a finding.

Remediation:

Configure the SUSE operating system to prevent USB mass storage devices from automounting when connected to the host.

Add or update the following line to the "/etc/modprobe.d/50-blacklist.conf" file:

```
blacklist usb-storage
```

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

1.59 SLES-15-010490 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

If Network Security Services (NSS) is being used by the SUSE operating system it must prohibit the use of cached authentications after one day.

```
GROUP ID: V-234857
RULE ID: SV-234857r958828
```

Rationale:

If cached authentication information is out of date, the validity of the authentication information may be questionable.

Audit:

If NSS is not used on the operating system, this is Not Applicable.

If NSS is used by the SUSE operating system, verify it prohibits the use of cached authentications after one day.

Check that cached authentications cannot be used after one day with the following command:

```
sudo grep -i "memcache_timeout" /etc/sssd/sssd.conf

memcache_timeout = 86400
```

If "memcache_timeout" has a value greater than "86400", or is missing, this is a finding.

Remediation:

Configure NSS, if used by the SUSE operating system, to prohibit the use of cached authentications after one day.

Add or change the following line in "/etc/sssd/sssd.conf" just below the line "[nss]":

```
memcache_timeout = 86400
```

Additional Information:

CCI-002007 Prohibit the use of cached authenticators after an organization-defined time period.

- NIST SP 800-53 Revision 4::IA-5 (13)
- NIST SP 800-53 Revision 5::IA-5 (13)

1.60 SLES-15-010500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must configure the Linux Pluggable Authentication Modules (PAM) to prohibit the use of cached offline authentications after one day.

```
GROUP ID: V-234858
RULE ID: SV-234858r958828
```

Rationale:

If cached authentication information is out of date, the validity of the authentication information may be questionable.

Audit:

If SSSD is not being used on the operating system, this is Not Applicable.

Verify that the SUSE operating system PAM prohibits the use of cached off line authentications after one day.

Check that cached off line authentications cannot be used after one day with the following command:

```
sudo grep "offline_credentials_expiration" /etc/sssd/sssd.conf

offline_credentials_expiration = 1
```

If "offline_credentials_expiration" is not set to a value of "1", this is a finding.

Remediation:

Configure the SUSE operating system PAM to prohibit the use of cached authentications after one day.

Add or change the following line in "/etc/sssd/sssd.conf" just below the line "[pam]":

```
offline_credentials_expiration = 1
```

Additional Information:

CCI-002007 Prohibit the use of cached authenticators after an organization-defined time period.

- NIST SP 800-53 Revision 4::IA-5 (13)
- NIST SP 800-53 Revision 5::IA-5 (13)

1.61 SLES-15-010510 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

FIPS 140-2 mode must be enabled on the SUSE operating system.

```
GROUP ID: V-234859
RULE ID: SV-234859r987791
```

Rationale:

Use of weak or untested encryption algorithms undermines the purposes of using encryption to protect data. The SUSE operating system must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Satisfies: SRG-OS-000396-GPOS-00176, SRG-OS-000478-GPOS-00223

Audit:

Verify the SUSE operating system is running in FIPS mode by running the following command.

```
cat /proc/sys/crypto/fips_enabled

1
```

If nothing is returned, the file does not exist, or the value returned is "0", this is a finding.

Remediation:

To configure the SUSE operating system to run in FIPS mode, add "fips=1" to the kernel parameter during the SUSE operating system install.

Enabling FIPS mode on a preexisting system involves a number of modifications to the SUSE operating system. Refer to section 9.1, "Crypto Officer Guidance", of the following document for installation guidance:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2435.pdf

Additional Information:

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

1.62 SLES-15-010530 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

All networked SUSE operating systems must have and implement SSH to protect the confidentiality and integrity of transmitted and received information, as well as information during preparation for transmission.

```
GROUP ID: V-234860
RULE ID: SV-234860r958908
```

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:

Note: If the system is not networked, this requirement is Not Applicable.

Verify that the SUSE operating system implements SSH to protect the confidentiality and integrity of transmitted and received information, as well as information during preparation for transmission.

Check that the OpenSSH package is installed on the SUSE operating system with the following command:

```
zypper info openssh | grep -i installed
```

If the OpenSSH package is not installed, this is a finding.

Check that the OpenSSH service active on the SUSE operating system with the following command:

```
systemctl status sshd.service | grep -i "active:"

Active: active (running) since Thu 2017-01-12 15:03:38 UTC; 1 months 4 days
ago
```

If OpenSSH service is not active, this is a finding.

Remediation:

Note: If the system is not networked, this requirement is Not Applicable.

Configure the SUSE operating system to implement SSH to protect the confidentiality and integrity of transmitted and received information, as well as information during preparation for transmission.

Install the OpenSSH package on the SUSE operating system with the following command:

```
sudo zypper in openssh
```

Enable the OpenSSH service to start automatically on reboot with the following command:

```
sudo systemctl enable sshd.service
```

For the changes to take effect immediately, start the service with the following command:

```
sudo systemctl restart 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

CCI-002420 Maintain the confidentiality and/or integrity of information during preparation for transmission.

- NIST SP 800-53 Revision 4::SC-8 (2)
- NIST SP 800-53 Revision 5::SC-8 (2)

CCI-002421 Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4::SC-8 (1)
- NIST SP 800-53 Revision 5::SC-8 (1)

CCI-002422 Maintain the confidentiality and/or integrity of information during reception.

- NIST SP 800-53 Revision 4::SC-8 (2)
- NIST SP 800-53 Revision 5::SC-8 (2)

1.63 SLES-15-010540 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must implement kptr-restrict to prevent the leaking of internal kernel addresses.

```
GROUP ID: V-234861
RULE ID: SV-234861r958928
```

Rationale:

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

Examples of attacks are buffer overflow attacks.

Audit:

Verify the SUSE operating system prevents leaking of internal kernel addresses.

Check that the SUSE operating system prevents leaking of internal kernel addresses by running the following command:

```
sudo sysctl kernel.kptr_restrict

kernel.kptr_restrict = 1
```

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

Remediation:

Configure the SUSE operating system to prevent leaking of internal kernel addresses by running the following command:

```
sudo sysctl -w kernel.kptr_restrict=1
```

If "1" is not the system's default value, add or update the following line in "/etc/sysctl.d/99-stig.conf":

```
sudo sh -c 'echo "kernel.kptr_restrict=1" >> /etc/sysctl.d/99-stig.conf'

sudo 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

1.64 SLES-15-010550 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Address space layout randomization (ASLR) must be implemented by the SUSE operating system to protect memory from unauthorized code execution.

```
GROUP ID: V-234862
RULE ID: SV-234862r958928
```

Rationale:

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

Examples of attacks are buffer overflow attacks.

Audit:

Verify the SUSE operating system implements ASLR.

Check that the SUSE operating system implements ASLR by running the following command:

```
sudo sysctl kernel.randomize_va_space

Kernel.randomize_va_space = 2
```

If the kernel parameter "randomize_va_space" is not equal to "2" or nothing is returned, this is a finding.

Remediation:

Configure the SUSE operating system to implement ASLR by running the following command as an administrator:

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

If "2" is not the system's default value, add or update the following line in "/etc/sysctl.d/99-stig.conf":

```
sudo sh -c 'echo "kernel.randomize_va_space=2" >> /etc/sysctl.d/99-stig.conf'

sudo 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

1.65 SLES-15-010560 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-234863
RULE ID: SV-234863r958936
```

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 SUSE operating system removes all outdated software components after updated version have been installed by running the following command:

```
grep -i upgraderemovedroppedpackages /etc/zypp/zypp.conf

solver.upgradeRemoveDroppedPackages = true
```

If "solver.upgradeRemoveDroppedPackages" is commented out, is set to "false", or is missing completely, this is a finding.

Remediation:

Configure the SUSE operating system to remove all outdated software components after an update by editing the following line in "/etc/zypp/zypp.conf" to match the one provided below:

```
solver.upgradeRemoveDroppedPackages = true
```

Additional Information:

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

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

1.66 SLES-15-010570 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must notify the System Administrator (SA) when Advanced Intrusion Detection Environment (AIDE) discovers anomalies in the operation of any security functions.

```
GROUP ID: V-234864
RULE ID: SV-234864r958948
```

Rationale:

If anomalies are not acted on, security functions may fail to secure the system.

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.

Notifications provided by information systems include messages to local computer consoles and/or hardware indications, such as lights.

This capability must take into account operational requirements for availability for selecting an appropriate response. The organization may choose to shut down or restart the information system upon security function anomaly detection.

Audit:

Verify the SUSE operating system notifies the SA when AIDE discovers anomalies in the operation of any security functions.

Check to see if the aide cron job sends an email when executed with the following command:

```
grep -i "aide" /etc/cron.*/aide 0 0 * * * /usr/sbin/aide --check | /bin/mail
-s "$HOSTNAME - Daily AIDE integrity check run"

root@example_server_name.mil
```

If the "aide" file does not exist under the "/etc/cron" directory structure or the cron job is not configured to execute a binary to send an email (such as "/bin/mail"), this is a finding.

Remediation:

Configure the SUSE operating system to notify the SA when AIDE discovers anomalies in the operation of any security functions.

Create the aide crontab file in "/etc/cron.daily" and add following command replacing the "[E-MAIL]" parameter with a proper email address for the SA:

```
0 0 * * * /usr/sbin/aide --check | /bin/mail -s "$HOSTNAME - Daily AIDE integrity check run" root@example_server_name.mil
```

Note: Per requirement SLES-15-010418, the "mailx" package must be installed on the system to enable email functionality.

Additional Information:

CCI-002702 Shut the system down, restart the system, and/or initiate organization-defined alternative action(s) when anomalies in the operation of the organization-defined security functions are discovered.

- NIST SP 800-53 Revision 4::SI-6 d
- NIST SP 800-53 Revision 5::SI-6 d

1.67 SLES-15-010580 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must off-load rsyslog messages for networked systems in real time and off-load standalone systems at least weekly.

```
GROUP ID: V-234865
RULE ID: SV-234865r1082187
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Audit:

Verify that the SUSE operating system must off-load rsyslog messages for networked systems in real time and off-load standalone systems at least weekly.

For stand-alone hosts, verify with the system administrator that the log files are off-loaded at least weekly.

For networked systems, check that rsyslog is sending log messages to a remote server with the following command:

```
sudo grep "\*.\*" /etc/rsyslog.conf | grep "@" | grep -v "^#"

*.*;mail.none;news.none @192.168.1.101:514
```

If any active message labels in the file do not have a line to send log messages to a remote server, this is a finding.

Remediation:

Configure the SUSE operating system to off-load rsyslog messages for networked systems in real time.

For stand-alone systems establish a procedure to off-load log messages at least once a week.

For networked systems add a "@[Log_Server_IP_Address]" option to every active message label in "/etc/rsyslog.conf" or in a file in "/etc/rsyslog.d/ that does not have one. Some examples are listed below:

```
*.*;mail.none;news.none -/var/log/messages
*.*;mail.none;news.none @192.168.1.101:514
```

An additional option is to capture all of the log messages and send them to a remote log host:

```
*.* @@loghost:514
```

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)

1.68 SLES-15-020000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must provision temporary accounts with an expiration date for 72 hours.

```
GROUP ID: V-234866
RULE ID: SV-234866r958364
```

Rationale:

If temporary user accounts remain active when no longer needed or for an excessive period, these accounts may be used to gain unauthorized access. To mitigate this risk, automated termination of all temporary accounts must be set upon account creation.

Temporary accounts are established as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation.

If temporary accounts are used, the SUSE operating system must be configured to automatically terminate these types of accounts after a DoD-defined time period of 72 hours.

To address access requirements, many SUSE operating systems may be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

Audit:

Verify that the SUSE operating system provisions temporary accounts with an expiration date for "72" hours.

Ask the System Administrator if any temporary accounts have been added to the system. For every existing temporary account, run the following command to obtain its account expiration information:

```
sudo chage -l system_account_name
```

Verify each of these accounts has an expiration date that is within "72" hours of its creation.

If any temporary accounts have no expiration date set or do not expire within "72" hours of their creation, this is a finding.

Remediation:

In the event temporary accounts are required, configure the SUSE operating system to terminate them after "72" hours.

For every temporary account, run the following command to set an expiration date on it, substituting "system_account_name" with the appropriate value:

```
sudo chage -E `date -d "+3 days" +%Y-%m-%d` system_account_name
date -d "+3 days" +%Y-%m-%d
```

sets the 72-hour expiration date for the account at the time the command is run.

Additional Information:

CCI-000016 Automatically remove or disable temporary and emergency accounts after an organization-defined time-period for each type of account.

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

1.69 SLES-15-020010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must lock an account after three consecutive invalid access attempts.

```
GROUP ID: V-234867
RULE ID: SV-234867r958388
```

Rationale:

By limiting the number of failed access 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.

The pam_tally2.so module maintains a count of attempted accesses. This includes user name entry into a logon field as well as password entry. With counting access attempts, it is possible to lock an account without presenting a password into the password field. This should be taken into consideration as it poses as an avenue for denial of service.

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

Audit:

Verify the SUSE operating system locks a user account after three consecutive failed access attempts until the locked account is released by an administrator.

Check that the system locks a user account after three consecutive failed login attempts using the following command:

```
grep pam_tally2.so /etc/pam.d/common-auth

auth required pam_tally2.so onerr=fail deny=3
```

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

If the line is missing "onerr=fail", this is a finding.

If the line has "deny" set to a value other than 1, 2, or 3, this is a finding.

Check that the system resets the failed login attempts counter after a successful login using the following command:

```
grep pam_tally2.so /etc/pam.d/common-account

account required pam_tally2.so
```

If the account option is missing, or commented out, this is a finding.

Remediation:

Configure the operating system to lock an account when three unsuccessful access attempts occur.

Modify the first line of the auth section "/etc/pam.d/common-auth" file to match the following lines:

```
auth required pam_tally2.so onerr=fail silent audit deny=3
```

Add or modify the following line in the /etc/pam.d/common-account file:

```
account required pam_tally2.so
```

Note: Manual changes to the listed files may be overwritten by the "pam-config" program. The "pam-config" program should not be used to update the configurations listed in this requirement.

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-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

1.70 SLES-15-020020 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

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

```
GROUP ID: V-234868
RULE ID: SV-234868r958398
```

Rationale:

SUSE operating system management includes the ability to control the number of users and user sessions that utilize a SUSE operating system. Limiting the number of allowed users and sessions per user is helpful in reducing the risks related to Denial-of-Service (DoS) attacks.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based on mission needs and the operational environment for each system.

Audit:

Verify the SUSE operating system limits the number of concurrent sessions to 10 for all accounts and/or account types by running the following command:

```
grep "maxlogins" /etc/security/limits.conf
```

The result must contain the following line:

```
* hard maxlogins 10
```

If the "maxlogins" item is missing, the line does not begin with a star symbol, or the value is not set to "10" or less, this is a finding.

Remediation:

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

Add the following line to the file "/etc/security/limits.conf":

```
* 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

1.71 SLES-15-020030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must implement multifactor authentication for access to privileged accounts via pluggable authentication modules (PAM).

```
GROUP ID: V-234869
RULE ID: SV-234869r1009617
```

Rationale:

Using an authentication device, such as a Common Access Card (CAC) or token that is separate from the information system, ensures that even if the information system is compromised, that compromise will not affect credentials stored on the authentication device.

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

A privileged account is defined as an information system account with authorizations of a privileged user.

Remote access is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-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-000068-GPOS-00036, SRG-OS-000105-GPOS-00052, SRG-OS-000106-GPOS-00053, SRG-OS-000107-GPOS-00054, SRG-OS-000108-GPOS-00055, SRG-OS-000375-GPOS-00160, SRG-OS-000376-GPOS-00161, SRG-OS-000377-GPOS-00162

Audit:

Verify the SUSE operating system implements multifactor authentication for remote access to privileged accounts via PAM.

Check that the "pam_pkcs11.so" option is configured in the "/etc/pam.d/common-auth" file with the following command:

```
grep pam_pkcs11.so /etc/pam.d/common-auth

auth sufficient pam_pkcs11.so
```

If "pam_pkcs11.so" is not set in "/etc/pam.d/common-auth", this is a finding.

Remediation:

Configure the SUSE operating system to implement multifactor authentication for remote access to privileged accounts via PAM.

Add or update "pam_pkcs11.so" in "/etc/pam.d/common-auth" to match the following line:

```
auth sufficient pam_pkcs11.so
```

Additional Information:
CCI-000187 For public key-based authentication, map the authenticated identity to the account of the individual or group.
- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (c)
- NIST SP 800-53 Revision 5::IA-5 (2) (a) (2)

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-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-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)

CCI-004047 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that the device meets organization-defined strength of mechanism requirements.
- NIST SP 800-53 Revision 5::IA-2 (6) (b)

CCI-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-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-001948 The information system implements multifactor authentication for remote access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access.
- NIST SP 800-53 Revision 4::IA-2 (11)

1.72 SLES-15-020040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must deny direct logons to the root account using remote access via SSH.

```
GROUP ID: V-234870
RULE ID: SV-234870r1009618
```

Rationale:

To ensure individual accountability and prevent unauthorized access, organizational users must be individually identified and authenticated.

A group authenticator is a generic account used by multiple individuals. Use of a group authenticator alone does not uniquely identify individual users. Examples of the group authenticator is the UNIX OS "root" user account, the Windows "Administrator" account, the "sa" account, or a "helpdesk" account.

For example, the UNIX and Windows SUSE operating systems offer a "switch user" capability, allowing users to authenticate with their individual credentials and, when needed, "switch" to the administrator role. This method provides for unique individual authentication prior to using a group authenticator.

Users (and any processes acting on behalf of users) need to be uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization, which outlines specific user actions that can be performed on the SUSE operating system without identification or authentication.

Requiring individuals to be authenticated with an individual authenticator prior to using a group authenticator allows for traceability of actions, as well as adding an additional level of protection of the actions that can be taken with group account knowledge.

Audit:

Verify the SUSE operating system denies direct logons to the root account using remote access via SSH.

Check that SSH denies any user trying to log on directly as root with the following command:

```
sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' | tr
'\n' ' ' | xargs sudo grep -iH '^\s*permitrootlogin'

PermitRootLogin no
```

If the "PermitRootLogin" keyword is set to "yes", is missing, or is commented out, this is a finding.

Remediation:

Configure the SUSE operating system to deny direct logons to the root account using remote access via SSH.

Edit the appropriate "/etc/ssh/sshd_config" file, add or uncomment the line for "PermitRootLogin" and set its value to "no" (this file may be named differently or be in a different location):

```
PermitRootLogin no
```

Additional Information:

CCI-004045 Require users to be individually authenticated before granting access to the shared accounts or resources.

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

CCI-000770 The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

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

1.73 SLES-15-020050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must disable account identifiers (individuals, groups, roles, and devices) after 35 days of inactivity after password expiration.

```
GROUP ID: V-234871
RULE ID: SV-234871r1009619
```

Rationale:

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

The SUSE operating system needs to track periods of inactivity and disable application identifiers after 35 days of inactivity.

Audit:

Verify the SUSE operating system disables account identifiers after 35 days of inactivity since the password expiration.

Check the account inactivity value by performing the following command:

```
sudo grep -i '^inactive' /etc/default/useradd

INACTIVE=35
```

If no output is produced, or if "INACTIVE" is not set to a value greater than "0" and less than or equal to "35", this is a finding.

Remediation:

Configure the SUSE operating system to disable account identifiers after 35 days of inactivity since the password expiration.

Run the following command to change the configuration for "useradd" to disable the account identifier after 35 days:

```
sudo useradd -D -f 35
```

DOD recommendation is 35 days, but a lower value greater than "0" is acceptable.

Additional Information:

CCI-003627 Disable accounts when the accounts have expired.

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

CCI-003628 Disable accounts when the accounts are no longer associated to a user.

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

CCI-000795 The organization manages information system identifiers by disabling the identifier after an organization-defined time period of inactivity.

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

1.74 SLES-15-020060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must never automatically remove or disable emergency administrator accounts.

```
GROUP ID: V-234872
RULE ID: SV-234872r958508
```

Rationale:

Emergency accounts are privileged accounts that are established in response to crisis situations where the need for rapid account activation is required. Therefore, emergency account activation may bypass normal account authorization processes. If these accounts are automatically disabled, system maintenance during emergencies may not be possible, thus adversely affecting system availability.

Emergency accounts are different from infrequently used accounts (i.e., local logon accounts used by the organization's system administrators when network or normal logon/access is not available). Infrequently used accounts are not subject to automatic termination dates. Emergency accounts are accounts created in response to crisis situations, usually for use by maintenance personnel. The automatic expiration or disabling time period may be extended as needed until the crisis is resolved; however, it must not be extended indefinitely. A permanent account should be established for privileged users who need long-term maintenance accounts.

To address access requirements the SUSE operating system can be integrated with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements.

Audit:

Verify the SUSE operating system is configured such that emergency administrator accounts are never automatically removed or disabled.

Note: Root is typically the "account of last resort" on a system and is also used as the example emergency administrator account. If another account is being used as the emergency administrator account, the command should be used against that account.

Check to see if the root account password or account expires with the following command:

```
sudo chage -l [Emergency_Administrator]

Password expires:never
```

If "Password expires" or "Account expires" is set to anything other than "never", this is a finding.

Remediation:

Configure the SUSE operating system to never automatically remove or disable emergency administrator accounts.

Replace "[Emergency_Administrator]" in the following command with the correct emergency administrator account. Run the following command as an administrator:

```
sudo chage -I -1 -M 99999 [Emergency_Administrator]
```

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)

1.75 SLES-15-020061 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-256982
RULE ID: SV-256982r958508
```

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)

1.76 SLES-15-020080 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The SUSE operating system must display the date and time of the last successful account logon upon logon.

```
GROUP ID: V-234873
RULE ID: SV-234873r991589
```

Rationale:

Providing users with feedback on when account accesses last occurred facilitates user recognition and reporting of unauthorized account use.

Audit:

Verify the SUSE operating system 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/login

session required pam_lastlog.so showfailed
```

If "pam_lastlog" is missing from "/etc/pam.d/login" file, the "silent" option is present, or the returned line is commented out, this is a finding.

Remediation:

Configure the SUSE operating system to provide users with feedback on when account accesses last occurred by setting the required configuration options in "/etc/pam.d/login".

Add the following line to the top of "/etc/pam.d/login":

```
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

1.77 SLES-15-020090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must not have unnecessary accounts.

```
GROUP ID: V-234874
RULE ID: SV-234874r991589
```

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 SUSE operating system accounts 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
...
games:x:12:100:Games account:/var/games:/bin/bash
```

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, this is a finding.

Remediation:

Configure the SUSE operating 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

1.78 SLES-15-020091 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must not have unnecessary account capabilities.

```
GROUP ID: V-234875
RULE ID: SV-234875r991589
```

Rationale:

Accounts providing no operational purpose provide additional opportunities for system compromise. Therefore all necessary non interactive accounts should not have an interactive shell assigned to them.

Audit:

Verify all non-interactive SUSE operating system accounts do not have an interactive shell assigned to them.

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:

```
awk -F: '($7 !~ "/sbin/nologin" && $7 !~ "/bin/false"){print $1 ":" $3 ":"
$7}' /etc/passwd

root:0:/bin/bash
nobody:65534:/bin/bash
```

If a non-interactive accounts such as "games" or "nobody" is listed with an interactive shell, this is a finding.

Remediation:

Configure the SUSE operating system so that all non-interactive accounts on the system have no interactive shell assigned to them.

Run the following command to disable the interactive shell for a specific non-interactive user account:

```
sudo usermod --shell /sbin/nologin nobody
```

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

1.79 SLES-15-020099 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-251723
RULE ID: SV-251723r991589
```

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. For compatibility with sudo versions prior to 1.9.1, #include and #includedir are also accepted. 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

1.80 SLES-15-020100 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The SUSE operating system root account must be the only account with unrestricted access to the system.

```
GROUP ID: V-234876
RULE ID: SV-234876r991589
```

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 SUSE operating system. Multiple accounts with a UID of "0" afford an opportunity for potential intruders to guess a password for a privileged account.

Audit:

Verify that the SUSE operating system root account is the only account with unrestricted access to the system.

Check the system for duplicate UID "0" assignments with the following command:

```
awk -F: '$3 == 0 {print $1}' /etc/passwd

root
```

If any accounts other than root have a UID of "0", this is a finding.

Remediation:

Change the UID of any account on the SUSE operating system, other than the root account, 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

1.81 SLES-15-020101 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must restrict privilege elevation to authorized personnel.

```
GROUP ID: V-234877
RULE ID: SV-234877r991589
```

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

1.82 SLES-15-020102 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must require reauthentication when using the "sudo" command.

```
GROUP ID: V-234878
RULE ID: SV-234878r1050789
```

Rationale:

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

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

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".

Additional Information:

CCI-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5::SC-11 b

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

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

1.83 SLES-15-020103 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-234879
RULE ID: SV-234879r991589
```

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 egrep -ir '(rootpw|targetpw|runaspw)' /etc/sudoers /etc/sudoers.d* |
grep -v '#'

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

If 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
```

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 SLES-15-020104 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-251724
RULE ID: SV-251724r1050789
```

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" are 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-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5::SC-11 b

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

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

1.85 SLES-15-020110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All SUSE operating system local interactive user accounts, upon creation, must be assigned a home directory.

```
GROUP ID: V-234880
RULE ID: SV-234880r991589
```

Rationale:

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

Audit:

Verify all SUSE operating system 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 SUSE 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

1.86 SLES-15-020120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must display the date and time of the last successful account logon upon an SSH logon.

```
GROUP ID: V-234881
RULE ID: SV-234881r991589
```

Rationale:

Providing users with feedback on when account accesses via SSH last occurred facilitates user recognition and reporting of unauthorized account use.

Audit:

Verify all remote connections via SSH to the SUSE operating system display 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:

```
sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' | tr
'\n' ' ' | xargs sudo grep -iH '^\s*printlastlog'

PrintLastLog yes
```

If the "PrintLastLog" keyword is set to "no", is missing, or is commented out, this is a finding.

Remediation:

Configure the SUSE operating system to provide users with feedback on when account accesses last occurred.

Add or edit the following lines in the "/etc/ssh/sshd_config" file:

```
PrintLastLog yes
```

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

1.87 SLES-15-020130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must enforce passwords that contain at least one uppercase character.

```
GROUP ID: V-234882
RULE ID: SV-234882r1009621
```

Rationale:

Use of a complex password helps 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 SUSE operating system enforces password complexity by requiring at least one uppercase character.

Check that the operating system enforces password complexity by requiring that at least one uppercase character be used by using the following command:

```
grep pam_cracklib.so /etc/pam.d/common-password

password requisite pam_cracklib.so ucredit=-1
```

If the command does not return anything, the returned line is commented out, or has a second column value different from "requisite", or does not contain "ucredit=-1", this is a finding.

Remediation:

Configure the SUSE operating system to enforce password complexity by requiring at least one uppercase character.

Edit "/etc/pam.d/common-password" and edit the line containing "pam_cracklib.so" to contain the option "ucredit=-1" after the third column.

Additional Information:

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

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

CCI-000192 The information system enforces password complexity by the minimum number of upper case characters used.

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

1.88 SLES-15-020140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must enforce passwords that contain at least one lowercase character.

```
GROUP ID: V-234883
RULE ID: SV-234883r1009622
```

Rationale:

Use of a complex password helps 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 SUSE operating system enforces password complexity by requiring that at least one lowercase character.

Check that the operating system enforces password complexity by requiring that at least one lowercase character be used by using the following command:

```
grep pam_cracklib.so /etc/pam.d/common-password

password requisite pam_cracklib.so lcredit=-1
```

If the command does not return anything, the returned line is commented out, or has a second column value different from "requisite", or does not contain "lcredit=-1", this is a finding.

Remediation:

Configure the SUSE operating system to enforce password complexity by requiring at least one lowercase character.

Edit "/etc/pam.d/common-password" and edit the line containing "pam_cracklib.so" to contain the option "lcredit=-1" after the third column.

Additional Information:

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

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

CCI-000193 The information system enforces password complexity by the minimum number of lower case characters used.

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

1.89 SLES-15-020150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must enforce passwords that contain at least one numeric character.

```
GROUP ID: V-234884
RULE ID: SV-234884r1009623
```

Rationale:

Use of a complex password helps 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 SUSE operating system enforces password complexity by requiring that at least one numeric character.

Check that the operating system enforces password complexity by requiring that at least one numeric character be used by using the following command:

```
grep pam_cracklib.so /etc/pam.d/common-password

password requisite pam_cracklib.so dcredit=-1
```

If the command does not return anything, the returned line is commented out, or has a second column value different from "requisite", or does not contain "dcredit=-1", this is a finding.

Remediation:

Configure the SUSE operating system to enforce password complexity by requiring at least one numeric character.

Edit "/etc/pam.d/common-password" and edit the line containing "pam_cracklib.so" to contain the option "dcredit=-1" after the third column.

Additional Information:

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

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

CCI-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)

1.90 SLES-15-020160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must require the change of at least eight of the total number of characters when passwords are changed.

```
GROUP ID: V-234885
RULE ID: SV-234885r1009624
```

Rationale:

If the SUSE operating system allows the user to consecutively reuse extensive portions of passwords, this increases the chances of password compromise by increasing the window of opportunity for attempts at guessing and brute-force attacks.

Audit:

Verify the SUSE operating system requires at least eight characters be changed between the old and new passwords during a password change.

Check that the operating system requires at least eight characters be changed between the old and new passwords during a password change by running the following command:

```
grep pam_cracklib.so /etc/pam.d/common-password

password requisite pam_cracklib.so difok=8
```

If the command does not return anything, the returned line is commented out, or has a second column value different from "requisite", or does not contain "difok", or the value is less than "8", this is a finding.

Remediation:

Configure the SUSE operating system to require at least eight characters be changed between the old and new passwords during a password change with the following command:

Edit "/etc/pam.d/common-password" and edit the line containing "pam_cracklib.so" to contain the option "difok=8" after the third column.

Additional Information:

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

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

CCI-000195 The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.

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

1.91 SLES-15-020170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must configure the Linux Pluggable Authentication Modules (PAM) to only store encrypted representations of passwords.

```
GROUP ID: V-234886
RULE ID: SV-234886r1009625
```

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.

Audit:

Verify the SUSE operating system configures the Linux PAM to only store encrypted representations of passwords. All account passwords must be hashed with SHA512 encryption strength.

Check that PAM is configured to create SHA512 hashed passwords by running the following command:

```
grep pam_unix.so /etc/pam.d/common-password

password required pam_unix.so sha512
```

If the command does not return anything or the returned line is commented out, has a second column value different from "required", or does not contain "sha512", this is a finding.

Remediation:

Configure the SUSE operating system Linux PAM to only store encrypted representations of passwords. All account passwords must be hashed with SHA512 encryption strength.

Edit "/etc/pam.d/common-password" and edit the line containing "pam_unix.so" to contain the SHA512 keyword after third column. Remove the "nullok" option.

Additional Information:

CCI-004062 For password-based authentication, store passwords using an approved salted key derivation function, preferably using a keyed hash.

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

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

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

1.92 SLES-15-020180 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must employ FIPS 140-2-approved cryptographic hashing algorithms for all stored passwords.

```
GROUP ID: V-234887
RULE ID: SV-234887r1009626
```

Rationale:

The system must use a strong hashing algorithm to store the password. The system must use a sufficient number of hashing rounds to ensure the required level of entropy.

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

Satisfies: SRG-OS-000073-GPOS-00041, SRG-OS-000120-GPOS-00061

Audit:

Verify the SUSE operating system requires the shadow password suite configuration be set to encrypt interactive user passwords using a strong cryptographic hash.

Check that the interactive user account passwords are using a strong password hash with the following command:

```
sudo cut -d: -f2 /etc/shadow

$6$kcOnRq/5$NUEYPuyL.wghQwWssXRcLRFiiru7f5JPV6GaJhNC2aK5F3PZpE/BCCtwrxRc/AInK
MNX3CdMw11m9STiql12f/
```

Password hashes "!" or "*" indicate inactive accounts not available for logon and are not evaluated.

If any interactive user password hash does not begin with "$6", this is a finding.

Remediation:

Configure the SUSE operating system to encrypt all stored passwords with a strong cryptographic hash.

Edit/modify the following line in the "/etc/login.defs" file and set "ENCRYPT_METHOD" to have a value of "SHA512".

```
ENCRYPT_METHOD SHA512
```

Lock all interactive user accounts not using SHA512 hashing until the passwords can be regenerated.

Additional Information:

CCI-004062 For password-based authentication, store passwords using an approved salted key derivation function, preferably using a keyed hash.

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

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

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)

1.93 SLES-15-020181 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

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

```
GROUP ID: V-251725
RULE ID: SV-251725r991589
```

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:

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

1.94 SLES-15-020190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must employ FIPS 140-3 approved cryptographic hashing algorithms for all stored passwords.

```
GROUP ID: V-234888
RULE ID: SV-234888r1044810
```

Rationale:

The system must use a strong hashing algorithm to store the password. The system must use a sufficient number of hashing rounds to ensure the required level of entropy.

Passwords need to be protected at all times, and encryption is the standard method for protecting passwords. If passwords are not encrypted, they can be plainly read (i.e., clear text) and easily compromised.

Satisfies: SRG-OS-000073-GPOS-00041, SRG-OS-000120-GPOS-00061

Audit:

Verify the SUSE operating system configures the shadow password suite configuration to encrypt passwords using a strong cryptographic hash.

Check that a minimum number of hash rounds is configured by running the following command:

```
egrep "^SHA_CRYPT_" /etc/login.defs
```

If only one of "SHA_CRYPT_MIN_ROUNDS" or "SHA_CRYPT_MAX_ROUNDS" is set, and this value is below "100000", this is a finding.

If both "SHA_CRYPT_MIN_ROUNDS" and "SHA_CRYPT_MAX_ROUNDS" are set, and the highest value for either is below "100000", this is a finding.

Remediation:

Configure the SUSE operating system to encrypt all stored passwords with a strong cryptographic hash.

Edit/modify the following line in the "/etc/login.defs" file and set "SHA_CRYPT_MIN_ROUNDS" to a value no lower than "100000":

```
SHA_CRYPT_MIN_ROUNDS 100000
```

Additional Information:

CCI-004062 For password-based authentication, store passwords using an approved salted key derivation function, preferably using a keyed hash.

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

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

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)

1.95 SLES-15-020200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must be configured to create or update passwords with a minimum lifetime of 24 hours (one day).

```
GROUP ID: V-234889
RULE ID: SV-234889r1009628
```

Rationale:

Enforcing a minimum password lifetime helps 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 SUSE operating system creates or updates passwords with minimum password age of one day or greater.

To check that the SUSE operating system enforces 24 hours/one day as the minimum password age, run the following command:

```
grep '^PASS_MIN_DAYS' /etc/login.defs

PASS_MIN_DAYS 1
```

If no output is produced, or if "PASS_MIN_DAYS" does not have a value of "1" or greater, this is a finding.

Remediation:

Configure the SUSE operating system to enforce 24 hours/one day or greater as the minimum password age.

Edit the file "/etc/login.defs" and add or correct the following line. Replace [DAYS] with the appropriate amount of days:

```
PASS_MIN_DAYS [DAYS]
```

The DOD requirement is "1" but a greater value is acceptable.

Additional Information:

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

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

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

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

1.96 SLES-15-020210 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must employ user passwords with a minimum lifetime of 24 hours (one day).

```
GROUP ID: V-234890
RULE ID: SV-234890r1009629
```

Rationale:

Enforcing a minimum password lifetime helps 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 SUSE operating system enforces a minimum time period between password changes for each user account of one day or greater.

Check the minimum time period between password changes for each user account with the following command:

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

smithj:1
```

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

Remediation:

Configure the SUSE operating system to enforce 24 hours/one day or greater as the minimum password age for user accounts.

Change the minimum time period between password changes for each [USER] account to "1" day with the command, replacing [USER] with the user account that must be changed:

```
sudo passwd -n 1 [USER]
```

Additional Information:

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

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

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

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

1.97 SLES-15-020220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must be configured to create or update passwords with a maximum lifetime of 60 days.

```
GROUP ID: V-234891
RULE ID: SV-234891r1038967
```

Rationale:

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

Audit:

Verify that the SUSE operating system is configured to create or update passwords with a maximum password age of 60 days or less.

Check that the SUSE operating system enforces 60 days or less as the maximum password age with the following command:

```
grep '^PASS_MAX_DAYS' /etc/login.defs
```

The DOD requirement is "60" days or less (greater than zero, as zero days will lock the account immediately).

If no output is produced, or if "PASS_MAX_DAYS" is not set to "60" days or less, this is a finding.

Remediation:

Configure the SUSE operating system to enforce a maximum password age of 60 days or less.

Edit the file "/etc/login.defs" and add or correct the following line. Replace [DAYS] with the appropriate amount of days:

```
PASS_MAX_DAYS [DAYS]
```

The DOD requirement is 60 days or less (greater than zero, as zero days will lock the account immediately).

Additional Information:

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

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

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

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

1.98 SLES-15-020230 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must employ user passwords with a maximum lifetime of 60 days.

```
GROUP ID: V-234892
RULE ID: SV-234892r1038967
```

Rationale:

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

Audit:

Verify that the SUSE operating system enforces a maximum user password age of 60 days or less.

Check that the SUSE operating system enforces 60 days or less as the maximum user password age with the following command:

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

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

Remediation:

Configure the SUSE operating system to enforce a maximum password age of each [USER] account to 60 days. The command in the check text will give a list of users that need to be updated to be in compliance:

```
sudo passwd -x 60 [USER]
```

The DOD requirement is 60 days.

Additional Information:

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

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

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

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

1.99 SLES-15-020260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must employ passwords with a minimum of 15 characters.

```
GROUP ID: V-234895
RULE ID: SV-234895r1009632
```

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 determine strength and how long it takes to crack a password. Use of more characters in a password helps exponentially increase the time and/or resources required to compromise the password.

Audit:

Verify the SUSE operating system enforces a minimum 15-character password length.

Check that the operating system enforces a minimum 15-character password length with the following command:

```
grep pam_cracklib.so /etc/pam.d/common-password

password requisite pam_cracklib.so minlen=15
```

If the command does not return anything, the returned line is commented out, or has a second column value different from "requisite", or does not contain "minlen" value, or the value is less than "15", this is a finding.

Remediation:

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

Edit "/etc/pam.d/common-password" and edit the line containing "pam_cracklib.so" to contain the option "minlen=15" after the third column.

The DOD standard requires a minimum 15-character password length.

Additional Information:

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

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

CCI-000205 The information system enforces minimum password length.

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

1.100 SLES-15-020270 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must enforce passwords that contain at least one special character.

```
GROUP ID: V-234896
RULE ID: SV-234896r1009633
```

Rationale:

Use of a complex password helps 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 in determining 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.

Special characters are not alphanumeric. Examples include: ~ ! @ # $ % ^ *.

Audit:

Verify the SUSE operating system enforces password complexity by requiring at least one special character.

Check that the operating system enforces password complexity by requiring at least one special character using the following command:

```
grep pam_cracklib.so /etc/pam.d/common-password

password requisite pam_cracklib.so ocredit=-1
```

If the command does not return anything, the returned line is commented out, or has a second column value different from "requisite", or does not contain "ocredit=-1", this is a finding.

Remediation:

Configure the SUSE operating system to enforce password complexity by requiring at least one special character.

Edit "/etc/pam.d/common-password" and edit the line containing "pam_cracklib.so" to contain the option "ocredit=-1" after the third column.

Additional Information:

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

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

CCI-001619 The information system enforces password complexity by the minimum number of special characters used.

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

1.101 SLES-15-020290 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must prevent the use of dictionary words for passwords.

```
GROUP ID: V-234897
RULE ID: SV-234897r991587
```

Rationale:

If the SUSE operating system allows the user to select passwords based on dictionary words, this increases the chances of password compromise by increasing the opportunity for successful guesses and brute-force attacks.

Audit:

Verify the SUSE operating system prevents the use of dictionary words for passwords.

Check that the SUSE operating system prevents the use of dictionary words for passwords with the following command:

```
grep pam_cracklib.so /etc/pam.d/common-password

password requisite pam_cracklib.so
```

If the command does not return anything, or the returned line is commented out, this is a finding.

Remediation:

Configure the SUSE operating system to prevent the use of dictionary words for passwords.

Edit "/etc/pam.d/common-password" and add the following line:

```
password requisite pam_cracklib.so
```

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 SLES-15-020300 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The SUSE operating system must not be configured to allow blank or null passwords.

```
GROUP ID: V-234898
RULE ID: SV-234898r991589
```

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.

Audit:

Verify the SUSE operating system is not configured to allow blank or null passwords.

Check that blank or null passwords cannot be used by running the following command:

```
grep pam_unix.so /etc/pam.d/* | grep nullok
```

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:

Configure the SUSE operating system to not allow blank or null passwords.

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

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 SLES-15-030000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd.

```
GROUP ID: V-234899
RULE ID: SV-234899r1009634
```

Rationale:

Once an attacker establishes initial access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to simply create a new account. Auditing of account creation mitigates this risk.

To address access requirements, many SUSE operating systems may be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Satisfies: SRG-OS-000004-GPOS-00004, SRG-OS-000239-GPOS-00089, SRG-OS-000240-GPOS-00090, SRG-OS-000241-GPOS-00091, SRG-OS-000274-GPOS-00104, SRG-OS-000275-GPOS-00105, SRG-OS-000276-GPOS-00106, SRG-OS-000277-GPOS-00107, SRG-OS-000303-GPOS-00120, SRG-OS-000463-GPOS-00207, SRG-OS-000304-GPOS-00121, SRG-OS-000470-GPOS-00214, SRG-OS-000476-GPOS-00221

Audit:

Verify the SUSE operating system generates an audit record when all modifications occur to the "/etc/passwd" file.

Check that the file is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/etc/passwd'

-w /etc/passwd -p wa -k account_mod
```

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

Note: The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record when all modifications to the "/etc/passwd" file occur.

Add or update the following rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/passwd -p wa -k account_mod
```

To reload the rules file, restart the audit daemon:

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

Additional Information:

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

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

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-002130 Automatically audit account enabling actions.

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

CCI-001683 The information system notifies organization-defined personnel or roles for account creation actions.

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

CCI-001684 The information system notifies organization-defined personnel or roles for account modification actions.

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

CCI-001685 The information system notifies organization-defined personnel or roles for account disabling actions.

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

CCI-001686 The information system notifies organization-defined personnel or roles for account removal actions.

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

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.

- NIST SP 800-53 Revision 4::AC-2 (4)

1.104 SLES-15-030010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/group.

```
GROUP ID: V-234900
RULE ID: SV-234900r1009635
```

Rationale:

Once an attacker establishes initial access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to simply create a new account. Auditing of account creation mitigates this risk.

To address access requirements, many SUSE operating systems may be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

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-000463-GPOS-00207, SRG-OS-000476-GPOS-00221

Audit:

Verify the SUSE operating system generates an audit record when modifications occur to the "/etc/group" file.

Check that the file is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/etc/group'

-w /etc/group -p wa -k account_mod
```

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

Note: The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record when all modifications to the "/etc/group" file occur.

Add or update the following rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/group -p wa -k account_mod
```

To reload the rules file, restart the audit daemon:

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::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-002130 Automatically audit account enabling actions.

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

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

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

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.

- NIST SP 800-53 Revision 4::AC-2 (4)

1.105 SLES-15-030020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow.

```
GROUP ID: V-234901
RULE ID: SV-234901r1009636
```

Rationale:

Once an attacker establishes initial access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to simply create a new account. Auditing of account creation mitigates this risk.

To address access requirements, many SUSE operating systems may be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

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-000463-GPOS-00207, SRG-OS-000476-GPOS-00221

Audit:

Verify the SUSE operating system generates an audit record when modifications occur to the "/etc/shadow" file.

Check that the file is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/etc/shadow'

-w /etc/shadow -p wa -k account_mod
```

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

Note: The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record when all modifications to the "/etc/shadow" file occur.

Add or update the following rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/shadow -p wa -k account_mod
```

To reload the rules file, restart the audit daemon:

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::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-002130 Automatically audit account enabling actions.

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

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

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

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.

- NIST SP 800-53 Revision 4::AC-2 (4)

1.106 SLES-15-030030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/security/opasswd.

```
GROUP ID: V-234902
RULE ID: SV-234902r1009637
```

Rationale:

Once an attacker establishes initial access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to simply create a new account. Auditing of account creation mitigates this risk.

To address access requirements, many SUSE operating systems may be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

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-000463-GPOS-00207, SRG-OS-000476-GPOS-00221

Audit:

Verify the SUSE operating system generates an audit record when modifications occur to the "/etc/security/opasswd" file.

Check that the file is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/etc/security/opasswd'

-w /etc/security/opasswd -p wa -k account_mod
```

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

Note: The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record when all modifications to the "/etc/security/opasswd" file occur.

Add or update the following rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/security/opasswd -p wa -k account_mod
```

To reload the rules file, restart the audit daemon:

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::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-002130 Automatically audit account enabling actions.

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

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

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

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.

- NIST SP 800-53 Revision 4::AC-2 (4)

1.107 SLES-15-030040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/gshadow.

```
GROUP ID: V-234903
RULE ID: SV-234903r958368
```

Rationale:

Once an attacker establishes initial access to a system, the attacker often attempts to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to simply create a new account. Auditing of account creation mitigates this risk.

To address access requirements, many SUSE operating systems may be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

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-000463-GPOS-00207, SRG-OS-000476-GPOS-00221

Audit:

Verify the SUSE operating system generates an audit record when all modifications occur to the "/etc/gshadow" file.

Check that the file is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/etc/gshadow'

-w /etc/gshadow -p wa -k account_mod
```

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

Notes:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record when all modifications to the "/etc/gshadow" file occur.

Add or update the following rule to "/etc/audit/rules.d/audit.rules":

```
-w /etc/gshadow -p wa -k account_mod
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

Additional Information:

CCI-000018 Automatically audit account creation actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::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-002130 Automatically audit account enabling actions.

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

1.108 SLES-15-030050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

SUSE operating system audit records must contain information to establish what type of events occurred, the source of events, where events occurred, and the outcome of events.

```
GROUP ID: V-234904
RULE ID: SV-234904r958412
```

Rationale:

Without establishing what type of events occurred, the source of events, where events occurred, and the outcome of events, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Associating event types with detected events in the SUSE operating system audit logs provides a means of investigating an attack, recognizing resource utilization or capacity thresholds, or identifying an improperly configured SUSE operating system.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000038-GPOS-00016, SRG-OS-000039-GPOS-00017, SRG-OS-000040-GPOS-00018, SRG-OS-000041-GPOS-00019, SRG-OS-000042-GPOS-00021, SRG-OS-000051-GPOS-00024, SRG-OS-000054-GPOS-00025, SRG-OS-000122-GPOS-00063, SRG-OS-000254-GPOS-00095, SRG-OS-000255-GPOS-00096, SRG-OS-000392-GPOS-00172

Audit:

Verify the SUSE operating system produces audit records.

Check that the SUSE operating system produces audit records by running the following command to determine the current status of the auditd service:

```
systemctl is-active auditd.service

active
systemctl is-enabled auditd.service

enabled
```

If the service is not active or not enabled, this is a finding.

Remediation:

Enable the SUSE operating system auditd service by performing the following commands:

```
sudo systemctl enable auditd.service
sudo systemctl start auditd.service
```

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-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-000133 Ensure that audit records containing information that establishes the source of 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 d

CCI-000134 Ensure that audit records containing information that establishes the outcome of 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 e

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-000154 Provide the capability to centrally review and analyze audit records from multiple components within the system.

- NIST SP 800-53::AU-6 (4)
- NIST SP 800-53A::AU-6 (4).1
- NIST SP 800-53 Revision 4::AU-6 (4)
- NIST SP 800-53 Revision 5::AU-6 (4)

CCI-000158 Provide the capability to process, sort, and search audit records for events of interest based on organization-defined audit fields within audit records.

- NIST SP 800-53::AU-7 (1)
- NIST SP 800-53A::AU-7 (1).1
- NIST SP 800-53 Revision 4::AU-7 (1)
- NIST SP 800-53 Revision 5::AU-7 (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-001876 Provide an audit reduction capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-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)

1.109 SLES-15-030060 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The SUSE operating system must generate audit records for all uses of the ssh-keysign command.

```
GROUP ID: V-234905
RULE ID: SV-234905r958412
```

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.

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

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "ssh-keysign" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/usr/lib/ssh/ssh-keysign'

-a always,exit -S all -F path=/usr/lib/ssh/ssh-keysign -F perm=x -F
auid>=1000 -F auid!=-1 -k privileged-ssh-keysign
```

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "ssh-keysign" command.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/lib/ssh/ssh-keysign -F perm=x -F auid>=1000 -F
auid!=4294967295 -k privileged-ssh-keysign
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.110 SLES-15-030070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the passwd command.

```
GROUP ID: V-234906
RULE ID: SV-234906r958412
```

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.

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

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "passwd" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/usr/bin/passwd'

-a always,exit -S all -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F
auid!=-1 -k privileged-passwd
```

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "passwd" command.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F
auid!=4294967295 -k privileged-passwd
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.111 SLES-15-030080 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The SUSE operating system must generate audit records for all uses of the gpasswd command.

```
GROUP ID: V-234907
RULE ID: SV-234907r958412
```

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.

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

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "gpasswd" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/usr/bin/gpasswd'

-a always,exit -S all -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F
auid!=-1 -k privileged-gpasswd
```

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "gpasswd" command.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/gpasswd -F perm=x -F auid>=1000 -F
auid!=4294967295 -k privileged-gpasswd
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.112 SLES-15-030090 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The SUSE operating system must generate audit records for all uses of the newgrp command.

```
GROUP ID: V-234908
RULE ID: SV-234908r958412
```

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.

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

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "newgrp" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/usr/bin/newgrp'

-a always,exit -S all -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F
auid!=-1 -k privileged-newgrp
```

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "newgrp" command.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/newgrp -F perm=x -F auid>=1000 -F
auid!=4294967295 -k privileged-newgrp
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.113 SLES-15-030100 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The SUSE operating system must generate audit records for a uses of the chsh command.

```
GROUP ID: V-234909
RULE ID: SV-234909r958412
```

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.

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

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "chsh" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/usr/bin/chsh'

-a always,exit -S all -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F
auid!=-1 -k privileged-chsh
```

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "chsh" command.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/chsh -F perm=x -F auid>=1000 -F
auid!=4294967295 -k privileged-chsh
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.114 SLES-15-030110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the unix_chkpwd or unix2_chkpwd commands.

```
GROUP ID: V-234910
RULE ID: SV-234910r958412
```

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-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for any use of the "unix_chkpwd" or "unix2_chkpwd" commands.

Check that the commands are being audited by performing the following command:

```
sudo auditctl -l | egrep -w "(unix_chkpwd|unix2_chkpwd)"

-a always,exit -S all -F path=/sbin/unix_chkpwd -F perm=x -F auid>=1000 -F
auid!=-1 -k privileged-unix-chkpwd
-a always,exit -S all -F path=/sbin/unix2_chkpwd -F perm=x -F auid>=1000 -F
auid!=-1 -k privileged-unix2-chkpwd
```

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "unix_chkpwd" and "unix2_chkpwd" commands.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/sbin/unix_chkpwd -F perm=x -F auid>=1000 -F
auid!=4294967295 -k privileged-unix-chkpwd
-a always,exit -F path=/sbin/unix2_chkpwd -F perm=x -F auid>=1000 -F
auid!=4294967295 -k privileged-unix2-chkpwd
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.115 SLES-15-030120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the chage command.

```
GROUP ID: V-234911
RULE ID: SV-234911r958412
```

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-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for any use of the "chage" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/usr/bin/chage'

-a always,exit -S all -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F
auid!=-1 -k privileged-chage
```

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "chage" command.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/chage -F perm=x -F auid>=1000 -F
auid!=4294967295 -k privileged-chage
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.116 SLES-15-030130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the crontab command.

```
GROUP ID: V-234912
RULE ID: SV-234912r958412
```

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-000037-GPOS-00015, SRG-OS-000042-GPOS-00020, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for any use of the "crontab" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/usr/bin/crontab'

-a always,exit -S all -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F
auid!=-1 -k privileged-crontab
```

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "crontab" command.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/crontab -F perm=x -F auid>=1000 -F
auid!=4294967295 -k privileged-crontab
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.117 SLES-15-030140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must audit all uses of the sudoers file and all files in the /etc/sudoers.d/ directory.

```
GROUP ID: V-234913
RULE ID: SV-234913r958412
```

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 that the file and directory is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/etc/sudoers'

-w /etc/sudoers -p wa -k privileged-actions
-w /etc/sudoers.d -p wa -k privileged-actions
```

If the commands do not return output that match the examples, this is a finding.

Notes:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE 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
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.118 SLES-15-030150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the creat, open, openat, open_by_handle_at, truncate, and ftruncate system calls.

```
GROUP ID: V-234914
RULE ID: SV-234914r958412
```

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-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000461-GPOS-00205, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "creat", "open", "openat", "open_by_handle_at", "truncate", and "ftruncate" system calls.

Check that the system calls are being audited by performing the following command:

```
sudo auditctl -l | grep 'open\|truncate\|creat'

-a always,exit -F arch=b32 -S
creat,open,openat,open_by_handle_at,truncate,ftruncate -F exit=-EPERM -F
auid>=1000 -F auid!=-1 -k perm_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!=-1 -k perm_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!=-1 -k perm_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!=-1 -k perm_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.

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "creat", "open", "openat", "open_by_handle_at", "truncate", and "ftruncate" system calls.

Add or update the following rules to "/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!=4294967295 -k perm_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!=4294967295 -k perm_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!=4294967295 -k perm_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!=4294967295 -k perm_access
```

To reload the rules file, restart the audit daemon:

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.119 SLES-15-030190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the setxattr, fsetxattr, lsetxattr, removexattr, fremovexattr, and lremovexattr system calls.

```
GROUP ID: V-234918
RULE ID: SV-234918r958412
```

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-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000466-GPOS-00210, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "setxattr", "fsetxattr", "lsetxattr", "removexattr", "fremovexattr", and "lremovexattr" system calls.

Check that the system calls are being audited by performing the following command:

```
sudo auditctl -l | grep xattr

-a always,exit -F arch=b32 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F
auid>=1000 -F auid!=-1 -k perm_mod
-a always,exit -F arch=b64 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F
auid>=1000 -F auid!=-1 -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.

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "setxattr", "fsetxattr", "lsetxattr","removexattr", "fremovexattr", and "lremovexattr" system calls.

Add or update the following rules to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F
auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S
setxattr,fsetxattr,lsetxattr,removexattr,fremovexattr,lremovexattr -F
auid>=1000 -F auid!=4294967295 -k perm_mod
```

To reload the rules file, restart the audit daemon:

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.120 SLES-15-030250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the chown, fchown, fchownat, and lchown system calls.

```
GROUP ID: V-234924
RULE ID: SV-234924r958412
```

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-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "chown", "fchown", "fchownat", and "lchown" system calls.

Check that the system calls are being audited by performing the following command:

```
sudo auditctl -l | grep chown

-a always,exit -F arch=b32 -S chown,fchown,fchownat,lchown -F auid>=1000 -F
auid!=-1 -k perm_mod
-a always,exit -F arch=b64 -S chown,fchown,fchownat,lchown -F auid>=1000 -F
auid!=-1 -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.

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "chown", "fchown", "fchownat", and "lchown" system calls.

Add or update the following rules to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S chown,fchown,fchownat,lchown -F auid>=1000 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chown,fchown,fchownat,lchown -F auid>=1000 -F
auid!=4294967295 -k perm_mod
```

To reload the rules file, restart the audit daemon:

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.121 SLES-15-030290 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the chmod, fchmod, and fchmodat system calls.

```
GROUP ID: V-234928
RULE ID: SV-234928r958412
```

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-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000064-GPOS-00033, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "chmod", "fchmod" a,nd "fchmodat" system calls.

Check that the system calls are being audited by performing the following command:

```
sudo auditctl -l | grep chmod

-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1
-k perm_mod
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1
-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.

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "chmod", "fchmod", and "fchmodat" system calls.

Add or update the following rules to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F
auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F
auid!=4294967295 -k perm_mod
```

To reload the rules file, restart the audit daemon:

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.122 SLES-15-030330 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the sudoedit command.

```
GROUP ID: V-234932
RULE ID: SV-234932r958412
```

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-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify an audit record is generated for all uses of the "sudoedit" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/usr/bin/sudoedit'

-a always,exit -S all -F path=/usr/bin/sudoedit -F perm=x -F auid>=1000 -F
auid!=-1 -k privileged-sudoedit
```

If the command does not return any output or the returned line is commented out, this is a finding.

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "sudoedit" command.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/sudoedit -F perm=x -F auid>=1000 -F
auid!=4294967295 -k privileged-sudoedit
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.123 SLES-15-030340 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The SUSE operating system must generate audit records for all uses of the chfn command.

```
GROUP ID: V-234933
RULE ID: SV-234933r958412
```

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.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "chfn" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/usr/bin/chfn'

-a always,exit -S all -F path=/usr/bin/chfn -F perm=x -F auid>=1000 -F
auid!=-1 -k privileged-chfn
```

If the command does not return any output or the returned line is commented out, this is a finding.

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "chfn" command.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/chfn -F perm=x -F auid>=1000 -F
auid!=4294967295 -k privileged-chfn
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.124 SLES-15-030350 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The SUSE operating system must generate audit records for all uses of the mount system call.

```
GROUP ID: V-234934
RULE ID: SV-234934r958412
```

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.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "mount" system call.

Check that the system call is being audited by performing the following command:

```
sudo auditctl -l | grep -w 'mount'

-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=-1 -k privileged-
mount
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=-1 -k privileged-
mount
```

If both the "b32" and "b64" audit rules are not defined for the "mount" syscall, this is a finding.

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "mount" system call.

Add or update the following rules to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k
privileged-mount
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k
privileged-mount
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.125 SLES-15-030360 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The SUSE operating system must generate audit records for all uses of the umount system call.

```
GROUP ID: V-234935
RULE ID: SV-234935r958412
```

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.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "umount" and "umount2" system calls.

Check that the system calls are being audited by performing the following command:

```
sudo auditctl -l | grep 'umount'

-a always,exit -F arch=b32 -S umount -F auid>=1000 -F auid!=-1 -k privileged-
umount
-a always,exit -F arch=b32 -S umount2 -F auid>=1000 -F auid!=-1 -k
privileged-umount
-a always,exit -F arch=b64 -S umount2 -F auid>=1000 -F auid!=-1 -k
privileged-umount
```

If both the "b32" and "b64" audit rules are not defined for the "umount" syscall, this is a finding.

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "umount" and "umount2" system calls.

Add or update the following rules to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S umount -F auid>=1000 -F auid!=4294967295 -k
privileged-umount
-a always,exit -F arch=b32 -S umount2 -F auid>=1000 -F auid!=4294967295 -k
privileged-umount
-a always,exit -F arch=b64 -S umount2 -F auid>=1000 -F auid!=4294967295 -k
privileged-umount
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.126 SLES-15-030370 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The SUSE operating system must generate audit records for all uses of the ssh-agent command.

```
GROUP ID: V-234936
RULE ID: SV-234936r958412
```

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.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "ssh-agent" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/usr/bin/ssh-agent'

-a always,exit -S all -F path=/usr/bin/ssh-agent -F perm=x -F auid>=1000 -F
auid!=-1 -k privileged-ssh-agent
```

If the command does not return any output or the returned line is commented out, this is a finding.

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "ssh-agent" command.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/ssh-agent -F perm=x -F auid>=1000 -F
auid!=4294967295 -k privileged-ssh-agent
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.127 SLES-15-030380 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the insmod command.

```
GROUP ID: V-234937
RULE ID: SV-234937r958412
```

Rationale:

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

Audit records can be generated from various components within the information system (e.g., module or policy filter).

The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records.

DoD has defined the following list of events for which the SUSE operating system will provide an audit record generation capability:

1. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels);
2. Access actions, such as successful and unsuccessful logon attempts, privileged activities or other system-level access, starting and ending time for user access to the system, concurrent logons from different workstations, successful and unsuccessful accesses to objects, all program initiations, and all direct access to the information system;
3. All account creations, modifications, disabling, and terminations; and
4. All kernel module load, unload, and restart actions.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system is generates an audit record for all uses of the "insmod" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/sbin/insmod'

-w /sbin/insmod -p x -k modules
```

If the system is configured to audit the execution of the module management program "insmod", the command will return a line.

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to audit the execution of the module management program "insmod" by adding the following line to "/etc/audit/rules.d/audit.rules":

```
-w /sbin/insmod -p x -k modules
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.128 SLES-15-030390 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the rmmod command.

```
GROUP ID: V-234938
RULE ID: SV-234938r958412
```

Rationale:

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

Audit records can be generated from various components within the information system (e.g., module or policy filter).

The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records.

DoD has defined the following list of events for which the SUSE operating system will provide an audit record generation capability:

1. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels);
2. Access actions, such as successful and unsuccessful logon attempts, privileged activities or other system-level access, starting and ending time for user access to the system, concurrent logons from different workstations, successful and unsuccessful accesses to objects, all program initiations, and all direct access to the information system;
3. All account creations, modifications, disabling, and terminations; and
4. All kernel module load, unload, and restart actions.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "rmmod" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/sbin/rmmod'

-w /sbin/rmmod -p x -k modules
```

If the system is configured to audit the execution of the module management program "rmmod", the command will return a line.

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to audit the execution of the module management program "rmmod" by adding the following line to "/etc/audit/rules.d/audit.rules":

```
-w /sbin/rmmod -p x -k modules
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.129 SLES-15-030400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the modprobe command.

```
GROUP ID: V-234939
RULE ID: SV-234939r958412
```

Rationale:

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

Audit records can be generated from various components within the information system (e.g., module or policy filter).

The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records.

DoD has defined the following list of events for which the SUSE operating system will provide an audit record generation capability:

1. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels);
2. Access actions, such as successful and unsuccessful logon attempts, privileged activities or other system-level access, starting and ending time for user access to the system, concurrent logons from different workstations, successful and unsuccessful accesses to objects, all program initiations, and all direct access to the information system;
3. All account creations, modifications, disabling, and terminations; and
4. All kernel module load, unload, and restart actions.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "modprobe" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/sbin/modprobe'

-w /sbin/modprobe -p x -k modules
```

If the system is configured to audit the execution of the module management program "modprobe", the command will return a line.

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to audit the execution of the module management program "modprobe" by adding the following line to "/etc/audit/rules.d/audit.rules":

```
-w /sbin/modprobe -p x -k modules
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.130 SLES-15-030410 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the kmod command.

```
GROUP ID: V-234940
RULE ID: SV-234940r958412
```

Rationale:

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

Audit records can be generated from various components within the information system (e.g., module or policy filter).

The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records.

DoD has defined the following list of events for which the SUSE operating system will provide an audit record generation capability:

1. Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels);
2. Access actions, such as successful and unsuccessful logon attempts, privileged activities or other system-level access, starting and ending time for user access to the system, concurrent logons from different workstations, successful and unsuccessful accesses to objects, all program initiations, and all direct access to the information system;
3. All account creations, modifications, disabling, and terminations; and
4. All kernel module load, unload, and restart actions.

Satisfies: SRG-OS-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "kmod" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/usr/bin/kmod'

-w /usr/bin/kmod -p x -k modules
```

If the system is configured to audit the execution of the module management program "kmod", the command will return a line.

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to audit the execution of the module management program "kmod" by adding the following line to "/etc/audit/rules.d/audit.rules":

```
-w /usr/bin/kmod -p x -k modules
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.131 SLES-15-030420 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the chmod command.

```
GROUP ID: V-234941
RULE ID: SV-234941r958412
```

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-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "chmod" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/usr/bin/chmod'

-a always,exit -S all -F path=/usr/bin/chmod -F perm=x -F auid>=1000 -F
auid!=-1 -k prim_mod
```

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "chmod" command.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/chmod -F perm=x -F auid>=1000 -F
auid!=4294967295 -k prim_mod
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.132 SLES-15-030430 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the setfacl command.

```
GROUP ID: V-234942
RULE ID: SV-234942r958412
```

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-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "setfacl" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/usr/bin/setfacl'

-a always,exit -S all -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F
auid!=-1 -k prim_mod
```

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "setfacl" command.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F
auid!=4294967295 -k prim_mod
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.133 SLES-15-030440 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the chacl command.

```
GROUP ID: V-234943
RULE ID: SV-234943r958412
```

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-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "chacl" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/usr/bin/chacl'

-a always,exit -S all -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F
auid!=-1 -k prim_mod
```

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "chacl" command.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F
auid!=4294967295 -k prim_mod
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.134 SLES-15-030450 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the chcon command.

```
GROUP ID: V-234944
RULE ID: SV-234944r958412
```

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-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "chcon" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/usr/bin/chcon'

-a always,exit -S all -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F
auid!=-1 -k prim_mod
```

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "chcon" command.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F
auid!=4294967295 -k prim_mod
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.135 SLES-15-030460 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the rm command.

```
GROUP ID: V-234945
RULE ID: SV-234945r958412
```

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-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "rm" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/usr/bin/rm'

-a always,exit -S all -F path=/usr/bin/rm -F perm=x -F auid>=1000 -F auid!=-1
-k prim_mod
```

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "rm" command.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/rm -F perm=x -F auid>=1000 -F
auid!=4294967295 -k prim_mod
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.136 SLES-15-030470 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all modifications to the tallylog file must generate an audit record.

```
GROUP ID: V-234946
RULE ID: SV-234946r958412
```

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-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000473-GPOS-00218

Audit:

Verify the SUSE operating system generates an audit record when all modifications to the "tallylog" file occur.

Check that the file is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/var/log/tallylog'

-w /var/log/tallylog -p wa -k logins
```

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for any all modifications to the "tallylog" file occur.

Add or update the following rule to "/etc/audit/rules.d/audit.rules":

```
-w /var/log/tallylog -p wa -k logins
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.137 SLES-15-030480 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all modifications to the lastlog file.

```
GROUP ID: V-234947
RULE ID: SV-234947r958412
```

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-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000473-GPOS-00218

Audit:

Verify the SUSE operating system generates an audit record when all modifications to the "lastlog" file occur.

Check that the file is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/var/log/lastlog'

-w /var/log/lastlog -p wa -k logins
```

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for any all modifications to the "lastlog" file occur.

Add or update the following rule to "/etc/audit/rules.d/audit.rules":

```
-w /var/log/lastlog -p wa -k logins
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.138 SLES-15-030490 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the passmass command.

```
GROUP ID: V-234948
RULE ID: SV-234948r958412
```

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-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "passmass" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/usr/bin/passmass'

-a always,exit -S all -F path=/usr/bin/passmass -F perm=x -F auid>=1000 -F
auid!=-1 -k privileged-passmass
```

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "passmass" command.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/passmass -F perm=x -F auid>=1000 -F
auid!=4294967295 -k privileged-passmass
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.139 SLES-15-030500 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the usermod command.

```
GROUP ID: V-234949
RULE ID: SV-234949r958412
```

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-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for any use of the "usermod" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/usr/sbin/usermod'

-a always,exit -S all -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F
auid!=-1 -k privileged-usermod
```

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "usermod" command.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F
auid!=4294967295 -k privileged-usermod
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.140 SLES-15-030510 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the pam_timestamp_check command.

```
GROUP ID: V-234950
RULE ID: SV-234950r958412
```

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-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215

Audit:

Verify the SUSE operating system generates an audit record for any use of the "pam_timestamp_check" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/sbin/pam_timestamp_check'

-a always,exit -S all -F path=/sbin/pam_timestamp_check -F perm=x -F
auid>=1000 -F auid!=-1 -k privileged-pam_timestamp_check
```

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

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "pam_timestamp_check" command.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/sbin/pam_timestamp_check -F perm=x -F auid>=1000 -F
auid!=4294967295 -k privileged-pam_timestamp_check
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.141 SLES-15-030520 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the delete_module system call.

```
GROUP ID: V-234951
RULE ID: SV-234951r958412
```

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-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "delete_module" system call.

Check that the system call is being audited by performing the following command:

```
sudo auditctl -l | grep -w 'delete_module'

-a always,exit -F arch=b32 -S delete_module -F auid>=1000 -F auid!=-1 -k
unload_module
-a always,exit -F arch=b64 -S delete_module -F auid>=1000 -F auid!=-1 -k
unload_module
```

If both the "b32" and "b64" audit rules are not defined for the "unload_module" syscall, this is a finding.

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "delete_module" system call.

Add or update the following rules to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S delete_module -F auid>=1000 -F auid!=4294967295
-k unload_module
-a always,exit -F arch=b64 -S delete_module -F auid>=1000 -F auid!=4294967295
-k unload_module
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.142 SLES-15-030530 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the init_module and finit_module system calls.

```
GROUP ID: V-234952
RULE ID: SV-234952r958412
```

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-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000471-GPOS-00216, SRG-OS-000477-GPOS-00222

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "init_module" and "finit_module" system calls.

Check that the system calls are being audited by performing the following command:

```
sudo auditctl -l | grep init_module

-a always,exit -F arch=b32 -S init_module,finit_module -F auid>=1000 -F
auid!=-1 -k moduleload
-a always,exit -F arch=b64 -S init_module,finit_module -F auid>=1000 -F
auid!=-1 -k moduleload
```

If both the "b32" and "b64" audit rules are not defined for the init_module" and "finit_module" syscalls, this is a finding.

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "init_module" and "finit_module" system calls.

Add or update the following rules to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S init_module,finit_module -F auid>=1000 -F
auid!=4294967295 -k moduleload
-a always,exit -F arch=b64 -S init_module,finit_module -F auid>=1000 -F
auid!=4294967295 -k moduleload
```

To reload the rules file, restart the audit daemon:

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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)

1.143 SLES-15-030550 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the su command.

```
GROUP ID: V-234954
RULE ID: SV-234954r958412
```

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-000037-GPOS-00015, SRG-OS-000062-GPOS-00031, SRG-OS-000392-GPOS-00172, SRG-OS-000462-GPOS-00206, SRG-OS-000471-GPOS-00215, SRG-OS-000042-GPOS-00020

Audit:

Verify the SUSE operating system generates an audit record for any use of the "su" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/usr/bin/su'

-a always,exit -S all -F path=/usr/bin/su -F perm=x -F auid>=1000 -F auid!=-1
-k privileged-priv_change
```

If the command does not return any output or the returned line is commented out, this is a finding.

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "su" command.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/su -F perm=x -F auid>=1000 -F
auid!=4294967295 -k privileged-priv_change
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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 SLES-15-030560 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The SUSE operating system must generate audit records for all uses of the sudo command.

```
GROUP ID: V-234955
RULE ID: SV-234955r958412
```

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.

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

Audit:

Verify the SUSE operating system generates an audit record for any use of the "sudo" command.

Check that the command is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/usr/bin/sudo'

-a always,exit -S all -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F
auid!=-1 -k privileged-sudo
```

If the command does not return any output, or the returned line is commented out, this is a finding.

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "sudo" command.

Add or update the following rules in the "/etc/audit/rules.d/audit.rules" file:

```
-a always,exit -F path=/usr/bin/sudo -F perm=x -F auid>=1000 -F
auid!=4294967295 -k privileged-sudo
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

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

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

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 SLES-15-030570 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Information System Security Officer (ISSO) and System Administrator (SA), at a minimum, must be alerted of a SUSE operating system audit processing failure event.

```
GROUP ID: V-234956
RULE ID: SV-234956r958424
```

Rationale:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Audit:

Verify the administrators are notified in the event of a SUSE operating system audit processing failure by inspecting "/etc/audit/auditd.conf".

Check if the system is configured to send email to an account when it needs to notify an administrator with the following command:

```
sudo grep action_mail /etc/audit/auditd.conf

action_mail_acct = root
```

If the value of the "action_mail_acct" keyword is not set to "root" and/or other accounts for security personnel, the "action_mail_acct" keyword is missing, or the returned line is commented out, this is a finding.

Remediation:

Configure the auditd service to notify the administrators in the event of a SUSE operating system audit processing failure.

Edit the following line in "/etc/audit/auditd.conf" to ensure that administrators are notified via email for those situations:

```
action_mail_acct = root
```

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

1.146 SLES-15-030580 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Information System Security Officer (ISSO) and System Administrator (SA), at a minimum, must have mail aliases to be notified of a SUSE operating system audit processing failure.

```
GROUP ID: V-234957
RULE ID: SV-234957r958424
```

Rationale:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability, and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

Audit:

Verify the administrators are notified in the event of a SUSE operating system audit processing failure by checking that "/etc/aliases" has a defined value for root.

```
grep -i "^postmaster:" /etc/aliases

postmaster: root
```

If the above command does not return a value of "root", or the output is commented out, this is a finding

Verify the alias for root forwards to a monitored e-mail account:

```
grep -i "^root:" /etc/aliases

root: person@server.mil
```

If the alias for root does not forward to a monitored e-mail account, or the output is commented out, this is a finding.

Remediation:

Configure the auditd service to notify the administrators in the event of a SUSE operating system audit processing failure.

Configure an alias value for the postmaster with the following command:

```
sudo sh -c 'echo "postmaster: root" >> /etc/aliases'
```

Configure an alias for root that forwards to a monitored email address with the following command:

```
sudo sh -c 'echo "root: box@server.mil" >> /etc/aliases'
```

The following command must be run to implement changes to the /etc/aliases file:

```
sudo newaliases
```

Additional Information:

CCI-000139 Alert organization-defined personnel or roles within an organization-defined time period in the event of an audit logging process failure.

- NIST SP 800-53::AU-5 a
- NIST SP 800-53A::AU-5.1 (ii)
- NIST SP 800-53 Revision 4::AU-5 a
- NIST SP 800-53 Revision 5::AU-5 a

1.147 SLES-15-030590 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system audit system must take appropriate action when the audit storage volume is full.

```
GROUP ID: V-234958
RULE ID: SV-234958r1038966
```

Rationale:

It is critical that when the SUSE operating system is at risk of failing to process audit logs as required, it takes action to mitigate the failure. Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Responses to audit failure depend on the nature of the failure mode.

When availability is an overriding concern, other approved actions in response to an audit failure are as follows:

1. If the failure was caused by the lack of audit record storage capacity, the SUSE operating system must continue generating audit records if possible (automatically restarting the audit service if necessary), overwriting the oldest audit records in a first-in-first-out manner.
2. If audit records are sent to a centralized collection server and communication with this server is lost or the server fails, the SUSE operating system must queue audit records locally until communication is restored or until the audit records are retrieved manually. Upon restoration of the connection to the centralized collection server, action should be taken to synchronize the local audit data with the collection server.

Audit:

Verify the SUSE operating system takes the appropriate action when the audit storage volume is full.

Check that the SUSE operating system takes the appropriate action when the audit storage volume is full with the following command:

```
sudo grep disk_full_action /etc/audit/auditd.conf

disk_full_action = SYSLOG
```

If the value of the "disk_full_action" option is not "SYSLOG", "SINGLE", or "HALT", or the line is commented out, this is a finding.

Remediation:

Configure the SUSE operating system to shut down by default upon audit failure (unless availability is an overriding concern).

Add or update the following line (depending on configuration "disk_full_action" can be set to "SYSLOG", "SINGLE", or "HALT" depending on configuration) in "/etc/audit/auditd.conf" file:

```
disk_full_action = HALT
```

Additional Information:

CCI-000140 Take organization-defined actions upon audit failure include, shutting down the system, overwriting oldest audit records, and stopping the generation of audit records.

- NIST SP 800-53::AU-5 b
- NIST SP 800-53A::AU-5.1 (iv)
- NIST SP 800-53 Revision 4::AU-5 b
- NIST SP 800-53 Revision 5::AU-5 b

1.148 SLES-15-030600 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must protect audit rules from unauthorized modification.

```
GROUP ID: V-234959
RULE ID: SV-234959r958434
```

Rationale:

Without the capability to restrict which roles and individuals can select which events are audited, unauthorized personnel may be able to prevent the auditing of critical events. Misconfigured audits may degrade the system's performance by overwhelming the audit log. Misconfigured audits may also make it more difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Satisfies: SRG-OS-000057-GPOS-00027, SRG-OS-000058-GPOS-00028, SRG-OS-000059-GPOS-00029

Audit:

Verify that the SUSE operating system protects audit rules from unauthorized modification.

Check that "permissions.local" file contains the correct permissions rules with the following command:

```
grep -i audit /etc/permissions.local

/var/log/audit root:root 600
/var/log/audit/audit.log root:root 600
/etc/audit/audit.rules root:root 640
/etc/audit/rules.d/audit.rules root:root 640
```

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

Check that all of the audit information files and folders have the correct permissions with the following command:

```
sudo chkstat /etc/permissions.local
```

If the command returns any output, this is a finding.

Remediation:

Configure the SUSE operating system to protect audit rules from unauthorized modification.

Add or update the following rules in "/etc/permissions.local":

```
/var/log/audit root:root 600
/var/log/audit/audit.log root:root 600
/etc/audit/audit.rules root:root 640
/etc/audit/rules.d/audit.rules root:root 640
```

Set the correct permissions with the following command:

```
sudo chkstat --set /etc/permissions.local
```

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

1.149 SLES-15-030620 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system audit tools must have the proper permissions configured to protect against unauthorized access.

```
GROUP ID: V-234961
RULE ID: SV-234961r991557
```

Rationale:

Protecting audit information also includes identifying and protecting the tools used to view and manipulate log data. Therefore, protecting audit tools is necessary to prevent unauthorized operation on audit information.

SUSE operating systems providing tools to interface with audit information will leverage user permissions and roles identifying the user accessing the tools and the corresponding rights the user enjoys to make access decisions regarding the access to audit tools.

Audit tools include but are not limited to vendor-provided and open-source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Satisfies: SRG-OS-000256-GPOS-00097, SRG-OS-000257-GPOS-00098, SRG-OS-000258-GPOS-00099

Audit:

Verify that the SUSE operating system audit tools have the proper permissions configured in the permissions profile to protect from unauthorized access.

Check that "permissions.local" file contains the correct permissions rules with the following command:

```
grep "^/usr/sbin/au" /etc/permissions.local

/usr/sbin/audispd root:root 0750
/usr/sbin/auditctl root:root 0750
/usr/sbin/auditd root:root 0750
/usr/sbin/ausearch root:root 0755
/usr/sbin/aureport root:root 0755
/usr/sbin/autrace root:root 0750
/usr/sbin/augenrules root:root 0750
```

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

Check that all of the audit information files and folders have the correct permissions with the following command:

```
sudo chkstat /etc/permissions.local
```

If the command returns any output, this is a finding.

Remediation:

Configure the SUSE operating system audit tools to have proper permissions set in the permissions profile to protect from unauthorized access.

Edit the file "/etc/permissions.local" and insert the following text:

```
/usr/sbin/audispd root:root 0750
/usr/sbin/auditctl root:root 0750
/usr/sbin/auditd root:root 0750
/usr/sbin/ausearch root:root 0755
/usr/sbin/aureport root:root 0755
/usr/sbin/autrace root:root 0750
/usr/sbin/augenrules root:root 0750
```

Set the correct permissions with the following command:

```
sudo chkstat --set /etc/permissions.local
```

Additional Information:

CCI-001493 Protect audit tools 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-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-001495 Protect audit tools 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

1.150 SLES-15-030630 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system file integrity tool must be configured to protect the integrity of the audit tools.

```
GROUP ID: V-234962
RULE ID: SV-234962r991567
```

Rationale:

Protecting the integrity of the tools used for auditing purposes is a critical step toward ensuring the integrity of audit information. Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Audit tools include but are not limited to vendor-provided and open-source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

It is not uncommon for attackers to replace the audit tools or inject code into the existing tools to provide the capability to hide or erase system activity from the audit logs.

To address this risk, audit tools must be cryptographically signed to provide the capability to identify when the audit tools have been modified, manipulated, or replaced. An example is a checksum hash of the file or files.

Audit:

Verify that the SUSE operating system file integrity tool is configured to protect the integrity of the audit tools.

Check that AIDE is properly configured to protect the integrity of the audit tools by running the following command:

```
sudo grep /usr/sbin/au /etc/aide.conf

/usr/sbin/auditctl p+i+n+u+g+s+b+acl+selinux+xattrs+sha512
/usr/sbin/auditd p+i+n+u+g+s+b+acl+selinux+xattrs+sha512
/usr/sbin/ausearch p+i+n+u+g+s+b+acl+selinux+xattrs+sha512
/usr/sbin/aureport p+i+n+u+g+s+b+acl+selinux+xattrs+sha512
/usr/sbin/autrace p+i+n+u+g+s+b+acl+selinux+xattrs+sha512
/usr/sbin/audispd p+i+n+u+g+s+b+acl+selinux+xattrs+sha512
/usr/sbin/augenrules p+i+n+u+g+s+b+acl+selinux+xattrs+sha512
```

If AIDE is properly configured to protect the integrity of the audit tools, all lines listed above will be returned from the command.

If one or more lines are missing, or is commented out, this is a finding.

Remediation:

Configure the SUSE operating system file integrity tool to protect the integrity of the audit tools.

Add or update the following lines to "/etc/aide.conf" to protect the integrity of the audit tools:

```
# audit tools
/usr/sbin/auditctl p+i+n+u+g+s+b+acl+selinux+xattrs+sha512
/usr/sbin/auditd p+i+n+u+g+s+b+acl+selinux+xattrs+sha512
/usr/sbin/ausearch p+i+n+u+g+s+b+acl+selinux+xattrs+sha512
/usr/sbin/aureport p+i+n+u+g+s+b+acl+selinux+xattrs+sha512
/usr/sbin/autrace p+i+n+u+g+s+b+acl+selinux+xattrs+sha512
/usr/sbin/audispd p+i+n+u+g+s+b+acl+selinux+xattrs+sha512
/usr/sbin/augenrules p+i+n+u+g+s+b+acl+selinux+xattrs+sha512
```

Additional Information:

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)

1.151 SLES-15-030640 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The SUSE operating system must generate audit records for all uses of the privileged functions.

```
GROUP ID: V-234963
RULE ID: SV-234963r1009638
```

Rationale:

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse and identify the risk from insider threats and the advanced persistent threat.

Satisfies: SRG-OS-000327-GPOS-00127, SRG-OS-000337-GPOS-00129, SRG-OS-000348-GPOS-00136, SRG-OS-000349-GPOS-00137, SRG-OS-000350-GPOS-00138, SRG-OS-000351-GPOS-00139, SRG-OS-000352-GPOS-00140, SRG-OS-000353-GPOS-00141, SRG-OS-000354-GPOS-00142, SRG-OS-000358-GPOS-00145, SRG-OS-000359-GPOS-00146, SRG-OS-000365-GPOS-00152

Audit:

Verify the SUSE operating system generates an audit record for any privileged use of the "execve" system call.

```
sudo auditctl -l | grep -w 'execve'

-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.

Note: The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for any privileged use of the "execve" system call.

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
```

To reload the rules file, restart the audit daemon:

```
sudo systemctl restart auditd.service
```

or issue the following command:

```
sudo augenrules --load
```

Additional Information:

CCI-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

CCI-001875 Provide an audit reduction capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001877 Provide an audit reduction capability that supports after-the-fact investigations of incidents.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001878 Provide a report generation capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001879 Provide a report generation capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001880 Provide a report generation capability that supports after-the-fact investigations of security incidents.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001881 Provide an audit reduction capability that does not alter original content or time ordering of audit records.

- NIST SP 800-53 Revision 4::AU-7 b
- NIST SP 800-53 Revision 5::AU-7 b

CCI-001882 Provide a report generation capability that does not alter original content or time ordering of audit records.

- NIST SP 800-53 Revision 4::AU-7 b
- NIST SP 800-53 Revision 5::AU-7 b

CCI-001889 Record time stamps for audit records that meet organization-defined granularity of time measurement.

- NIST SP 800-53 Revision 4::AU-8 b
- NIST SP 800-53 Revision 5::AU-8 b

CCI-001914 Provide the capability for organization-defined individuals or roles to change the logging to be performed on organization-defined system components based on organization-defined selectable event criteria within organization-defined time thresholds.

- NIST SP 800-53 Revision 4::AU-12 (3)
- NIST SP 800-53 Revision 5::AU-12 (3)

CCI-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)

CCI-001814 The Information system supports auditing of the enforcement actions.

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

1.152 SLES-15-030650 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must have the auditing package installed.

```
GROUP ID: V-234964
RULE ID: SV-234964r1009639
```

Rationale:

Without establishing what type of events occurred, the source of events, where events occurred, and the outcome of events, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit record content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Associating event types with detected events in the SUSE operating system audit logs provides a means of investigating an attack, recognizing resource utilization or capacity thresholds, or identifying an improperly configured SUSE operating system.

Satisfies: SRG-OS-000337-GPOS-00129, SRG-OS-000348-GPOS-00136, SRG-OS-000349-GPOS-00137, SRG-OS-000350-GPOS-00138, SRG-OS-000351-GPOS-00139, SRG-OS-000352-GPOS-00140, SRG-OS-000353-GPOS-00141, SRG-OS-000354-GPOS-00142, SRG-OS-000358-GPOS-00145, SRG-OS-000359-GPOS-00146, SRG-OS-000365-GPOS-00152, SRG-OS-000474-GPOS-00219, SRG-OS-000475-GPOS-00220

Audit:

Verify the SUSE operating system auditing package is installed.

Check that the "audit" package is installed by performing the following command:

```
zypper info audit | grep Installed

i | audit | User Space Tools for 2.6 Kernel Auditing
```

If the package "audit" is not installed on the system, then this is a finding.

Remediation:

The SUSE operating system auditd package must be installed on the system. If it is not installed, use the following command to install it:

```
sudo zypper in audit
```

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-003938 Automatically generate audit records of the enforcement actions.

- NIST SP 800-53 Revision 5::CM-5 (1) (b)

CCI-001875 Provide an audit reduction capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001877 Provide an audit reduction capability that supports after-the-fact investigations of incidents.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001878 Provide a report generation capability that supports on-demand audit review and analysis.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001879 Provide a report generation capability that supports on-demand reporting requirements.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001880 Provide a report generation capability that supports after-the-fact investigations of security incidents.

- NIST SP 800-53 Revision 4::AU-7 a
- NIST SP 800-53 Revision 5::AU-7 a

CCI-001881 Provide an audit reduction capability that does not alter original content or time ordering of audit records.

- NIST SP 800-53 Revision 4::AU-7 b
- NIST SP 800-53 Revision 5::AU-7 b

CCI-001882 Provide a report generation capability that does not alter original content or time ordering of audit records.

- NIST SP 800-53 Revision 4::AU-7 b
- NIST SP 800-53 Revision 5::AU-7 b

CCI-001889 Record time stamps for audit records that meet organization-defined granularity of time measurement.

- NIST SP 800-53 Revision 4::AU-8 b
- NIST SP 800-53 Revision 5::AU-8 b

CCI-001914 Provide the capability for organization-defined individuals or roles to change the logging to be performed on organization-defined system components based on organization-defined selectable event criteria within organization-defined time thresholds.

- NIST SP 800-53 Revision 4::AU-12 (3)
- NIST SP 800-53 Revision 5::AU-12 (3)

CCI-001814 The Information system supports auditing of the enforcement actions.

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

1.153 SLES-15-030670 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The audit-audispd-plugins must be installed on the SUSE operating system.

```
GROUP ID: V-234966
RULE ID: SV-234966r1009564
```

Rationale:

The audit-audispd-plugins must be installed on the SUSE operating system.

Audit:

Verify that the "audit-audispd-plugins" package is installed on the SUSE operating system.

Check that the "audit-audispd-plugins" package is installed on the SUSE operating system with the following command:

```
zypper info audit-audispd-plugins | grep Installed
```

If the "audit-audispd-plugins" package is not installed, this is a finding.

Remediation:

Install the "audit-audispd-plugins" package on the SUSE operating system by running the following command:

```
sudo zypper install audit-audispd-plugins
```

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

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

1.154 SLES-15-030680 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The SUSE operating system audit event multiplexor must be configured to use Kerberos.

```
GROUP ID: V-234967
RULE ID: SV-234967r1009567
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Allowing devices and users to connect to or from the system without first authenticating them allows untrusted access and can lead to a compromise or attack. Audit events that may include sensitive data must be encrypted prior to transmission. Kerberos provides a mechanism to provide both authentication and encryption for audit event records.

Audit:

Determine if the SUSE operating system audit event multiplexor is configured to use Kerberos by running the following command:

```
sudo grep transport /etc/audit/audisp-remote.conf

transport = krb5
```

If "transport" is not set to "krb5", or is commented out, this is a finding.

Remediation:

Configure the SUSE operating system audit event multiplexor to use Kerberos by editing the "/etc/audit/audisp-remote.conf" file.

Edit or add the following line to match the text below:

```
transport = krb5
```

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)

1.155 SLES-15-030660 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must allocate audit record storage capacity to store at least one week of audit records when audit records are not immediately sent to a central audit record storage facility.

```
GROUP ID: V-234965
RULE ID: SV-234965r958752
```

Rationale:

To ensure SUSE operating systems have a sufficient storage capacity in which to write the audit logs, SUSE operating systems need to be able to allocate audit record storage capacity.

The task of allocating audit record storage capacity is usually performed during initial installation of the SUSE operating system.

Audit:

Verify the SUSE operating system allocates audit record storage capacity to store at least one week of audit records when audit records are not immediately sent to a central audit record storage facility.

Determine to which partition the audit records are being written with the following command:

```
sudo grep -iw log_file /etc/audit/auditd.conf

log_file = /var/log/audit/audit.log
```

Check the size of the partition that audit records are written to (with the example being /var/log/audit/) with the following command:

```
df -h /var/log/audit/

/dev/sda2 24G 10.4G 13.6G 43% /var
```

If the audit records are not written to a partition made specifically for audit records (/var/log/audit is a separate partition), determine the amount of space being used by other files in the partition with the following command:

```
sudo du -sh [audit_partition]

1.8G /var/log/audit
```

The partition size needed to capture a week of audit records is based on the activity level of the system and the total storage capacity available. In normal circumstances, 10.0 GB of storage space for audit records will be sufficient.

If the audit record partition is not allocated sufficient storage capacity, this is a finding.

Remediation:

Allocate enough storage capacity for at least one week of SUSE operating system audit records when audit records are not immediately sent to a central audit record storage facility.

If audit records are stored on a partition made specifically for audit records, use the "YaST2 - Partitioner" program (installation and configuration tool for Linux) to resize the partition with sufficient space to contain one week of audit records.

If audit records are not stored on a partition made specifically for audit records, a new partition with sufficient amount of space will need be to be created. The new partition can be created using the "YaST2 - Partitioner" program on the system.

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

1.156 SLES-15-030690 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Audispd must off-load audit records onto a different system or media from the SUSE operating system being audited.

```
GROUP ID: V-234968
RULE ID: SV-234968r1009570
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Audit:

Verify "audispd" off-loads audit records onto a different system or media from the SUSE operating system being audited.

Check if "audispd" is configured to off-load audit records onto a different system or media from the SUSE operating system by running the following command:

```
sudo grep remote_server /etc/audit/audisp-remote.conf

remote_server = 192.168.1.101
```

If "remote_server" is not set to an external server or media, or is commented out, this is a finding.

Remediation:

Configure the SUSE operating system "/etc/audit/audisp-remote.conf" file to off-load audit records onto a different system or media by adding or editing the following line with the correct IP address:

```
remote_server = [IP ADDRESS]
```

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)

1.157 SLES-15-030700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system auditd service must notify the System Administrator (SA) and Information System Security Officer (ISSO) immediately when audit storage capacity is 75 percent full.

```
GROUP ID: V-234969
RULE ID: SV-234969r971542
```

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:

Determine if the SUSE operating system auditd is configured to notify the SA and ISSO when the audit record storage volume reaches 75 percent of the storage capacity.

Check the system configuration to determine the partition to which audit records are written using the following command:

```
sudo grep -iw log_file /etc/audit/auditd.conf

log_file = /var/log/audit/audit.log
```

Check the size of the partition to which audit records are written (e.g., "/var/log/audit/"):

```
df -h /var/log/audit/

/dev/sda2 24G 10.4G 13.6G 43% /var
```

If the audit records are not being written to a partition specifically created for audit records (in this example "/var/log/audit" is a separate partition), use the following command to determine the amount of space other files in the partition currently occupy:

```
sudo du -sh <partition>

1.8G /var/log/audit
```

Determine the threshold 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 = 225
```

If the value of the "space_left" keyword is not set to 25 percent of the total partition size, this is a finding.

Remediation:

Check the system configuration to determine the partition to which the audit records are written:

```
sudo grep -iw log_file /etc/audit/auditd.conf
```

Determine the size of the partition to which audit records are written (e.g., "/var/log/audit/"):

```
df -h /var/log/audit/
```

Set the value of the "space_left" keyword in "/etc/audit/auditd.conf" to 25 percent of the partition size.

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)

1.158 SLES-15-030760 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for the /run/utmp file.

```
GROUP ID: V-234975
RULE ID: SV-234975r991581
```

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 SUSE operating system generates an audit record for the "/run/utmp" file.

Check that the file is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/run/utmp'

-w /run/utmp -p wa -k login_mod
```

If the command does not return a line that match the example, this is a finding.

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for the "/run/utmp" file.

Add or update the following rules to "/etc/audit/rules.d/audit.rules":

```
-w /run/utmp -p wa -k login_mod
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue 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

1.159 SLES-15-030740 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for all uses of the unlink, unlinkat, rename, renameat, and rmdir system calls.

```
GROUP ID: V-234973
RULE ID: SV-234973r991577
```

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.

Audit:

Verify the SUSE operating system generates an audit record for all uses of the "unlink", "unlinkat", "rename", "renameat", and "rmdir" system calls.

Check that the system calls are being audited by performing the following command:

```
sudo auditctl -l | grep 'unlink\|rename\|rmdir'

-a always,exit -F arch=b32 -S unlink,unlinkat,rename,renameat,rmdir -F
auid>=1000 -F auid!=-1 -k perm_mod
-a always,exit -F arch=b64 -S unlink,unlinkat,rename,renameat,rmdir -F
auid>=1000 -F auid!=-1 -k perm_mod
```

If both the "b32" and "b64" audit rules are not defined for the "unlink", "unlinkat", "rename", "renameat", and "rmdir" syscalls, this is a finding.

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for all uses of the "unlink", "unlinkat", "rename", "renameat", and "rmdir" system calls.

Add or update the following rules to "/etc/audit/rules.d/audit.rules":

```
-a always,exit -F arch=b32 -S unlink,unlinkat,rename,renameat,rmdir -F
auid>=1000 -F auid!=4294967295 -k perm_mod
-a always,exit -F arch=b64 -S unlink,unlinkat,rename,renameat,rmdir -F
auid>=1000 -F auid!=4294967295 -k perm_mod
```

To reload the rules file, restart the audit daemon:

```
sudo systemctl restart auditd.service
```

or issue 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

1.160 SLES-15-030770 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for the /var/log/wtmp file.

```
GROUP ID: V-234976
RULE ID: SV-234976r991581
```

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 SUSE operating system generates an audit record for the "/var/log/wtmp" file.

Check that the file is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/var/log/wtmp'

-w /var/log/wtmp -p wa -k login_mod
```

If the command does not return a line that matches the example, this is a finding.

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for the "/var/log/wtmp" file.

Add or update the following rules to "/etc/audit/rules.d/audit.rules":

```
-w /var/log/wtmp -p wa -k login_mod
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue 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

1.161 SLES-15-030780 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must generate audit records for the /var/log/btmp file.

```
GROUP ID: V-234977
RULE ID: SV-234977r991581
```

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 SUSE operating system generates an audit record for the "/var/log/btmp" file.

Check that the file is being audited by performing the following command:

```
sudo auditctl -l | grep -w '/var/log/btmp'

-w /var/log/btmp -p wa -k login_mod
```

If the command does not return a line that matches the example, this is a finding.

Note:

The "-k" allows for specifying an arbitrary identifier. The string following "-k" does not need to match the example output above.

Remediation:

Configure the SUSE operating system to generate an audit record for the "/var/log/btmp" file.

Add or update the following rules to "/etc/audit/rules.d/audit.rules":

```
-w /var/log/btmp -p wa -k login_mod
```

To reload the rules file, restart the audit daemon

```
sudo systemctl restart auditd.service
```

or issue 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

1.162 SLES-15-030790 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must off-load audit records onto a different system or media from the system being audited.

```
GROUP ID: V-234978
RULE ID: SV-234978r1009573
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Audit:

Verify what action the audit system takes if it cannot off-load audit records to a different system or storage media from the SUSE operating system being audited.

Check the action that the audit system takes in the event of a network failure with the following command:

```
sudo grep -i "network_failure_action" /etc/audit/audisp-remote.conf

network_failure_action = syslog
```

If the "network_failure_action" option is not set to "syslog", "single", or "halt" or the line is commented out, this is a finding.

Remediation:

Configure the SUSE operating system to take the appropriate action if it cannot off-load audit records to a different system or storage media from the system being audited due to a network failure.

Uncomment the "network_failure_action" option in "/etc/audit/audisp-remote.conf" and set it to "syslog", "single", or "halt". See the example below:

```
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)

1.163 SLES-15-030800 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Audispd must take appropriate action when the SUSE operating system audit storage is full.

```
GROUP ID: V-234979
RULE ID: SV-234979r1009576
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Audit:

Verify the audit system off-loads audit records if the SUSE operating system storage volume becomes full.

Check that the records are properly off-loaded to a remote server with the following command:

```
sudo grep -i "disk_full_action" /etc/audit/audisp-remote.conf

disk_full_action = syslog
```

If "disk_full_action" is not set to "syslog", "single", or "halt" or the line is commented out, this is a finding.

Remediation:

Configure the SUSE operating system to take the appropriate action if the audit storage is full.

Add, edit, or uncomment the "disk_full_action" option in "/etc/audit/audisp-remote.conf". Set it to "syslog", "single" or "halt" as in the example below:

```
disk_full_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)

1.164 SLES-15-030810 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The SUSE operating system must use a separate file system for the system audit data path.

```
GROUP ID: V-234980
RULE ID: SV-234980r991589
```

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 the SUSE operating system has a separate file system/partition for the system audit data path.

Check that a file system/partition has been created for the system audit data path with the following command:

Note: "/var/log/audit" is used as the example as it is a common location.

```
grep /var/log/audit /etc/fstab

UUID=3645951a /var/log/audit ext4 defaults 1 2
```

If a separate entry for the system audit data path (in this example the "/var/log/audit" path) does not exist, ask the System Administrator if the system audit logs are being written to a different file system/partition on the system and then grep for that file system/partition.

If a separate file system/partition does not exist for the system audit data path, this is a finding.

Remediation:

Migrate the SUSE operating system audit data 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

1.165 SLES-15-030820 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must not disable syscall auditing.

```
GROUP ID: V-234981
RULE ID: SV-234981r991589
```

Rationale:

By default, the SUSE operating system includes the "-a task,never" audit rule as a default. This rule suppresses syscall auditing for all tasks started with this rule in effect. Because the audit daemon processes the "audit.rules" file from the top down, this rule supersedes all other defined syscall rules; therefore no syscall auditing can take place on the operating system.

Audit:

Verify syscall auditing has not been disabled:

```
auditctl -l | grep -i "a task,never"
```

If any results are returned, this is a finding.

Verify the default rule "-a task,never" is not statically defined :

```
grep -rv "^#" /etc/audit/rules.d/ | grep -i "a task,never"
```

If any results are returned, this is a finding.

Remediation:

Remove the "-a task,never" rule from the /etc/audit/rules.d/audit.rules file.

The audit daemon must be restarted for the changes to take effect.

```
sudo systemctl restart auditd.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

1.166 SLES-15-040000 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must enforce a delay of at least four seconds between logon prompts following a failed logon attempt.

```
GROUP ID: V-234982
RULE ID: SV-234982r991588
```

Rationale:

Limiting the number of logon attempts over a certain time interval reduces the chances that an unauthorized user may gain access to an account.

Audit:

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

Check that the SUSE operating system enforces a delay of at least four seconds between logon prompts following a failed logon attempt with the following command:

```
grep FAIL_DELAY /etc/login.defs

FAIL_DELAY 4
```

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

Remediation:

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

Add or update the following variable in "/etc/login.defs" to match the line below ("FAIL_DELAY" must have a value of "4" or higher):

```
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

1.167 SLES-15-040010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must enforce a delay of at least four seconds between logon prompts following a failed logon attempt.

```
GROUP ID: V-234983
RULE ID: SV-234983r991588
```

Rationale:

The SUSE operating system must enforce a delay of at least four seconds between logon prompts following a failed logon attempt.

Audit:

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

```
grep pam_faildelay /etc/pam.d/common-auth

auth required pam_faildelay.so delay=4000000
```

If the value of "delay" is not set to "4000000", "delay" is commented out, "delay" is missing, or the "pam_faildelay" line is missing completely, this is a finding.

Remediation:

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

Edit the file "/etc/pam.d/common-auth".

Add a parameter "pam_faildelay" and set it to:

delay is in micro seconds

```
auth required pam_faildelay.so delay=4000000
```

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

1.168 SLES-15-040020 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

There must be no .shosts files on the SUSE operating system.

```
GROUP ID: V-234984
RULE ID: SV-234984r991589
```

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 SUSE operating system.

Check the system for the existence of these files with the following command:

```
sudo find / \( -path /.snapshots -o -path /sys -o -path /proc \) -prune -o -
name '.shosts' -print
```

If any ".shosts" files are found on the system, this is a finding.

Remediation:

Remove any ".shosts" files found on the SUSE operating system.

```
sudo rm /[path]/[to]/[file]/.shosts
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.169 SLES-15-040030 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

There must be no shosts.equiv files on the SUSE operating system.

```
GROUP ID: V-234985
RULE ID: SV-234985r991589
```

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 SUSE operating system.

Check the system for the existence of these files with the following command:

```
sudo find /etc -name shosts.equiv
```

If any "shosts.equiv" files are found on the system, this is a finding.

Remediation:

Remove any "shosts.equiv" files found on the SUSE operating system.

```
sudo rm /[path]/[to]/[file]/shosts.equiv
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.170 SLES-15-040040 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The SUSE operating system file integrity tool must be configured to verify Access Control Lists (ACLs).

```
GROUP ID: V-234986
RULE ID: SV-234986r991589
```

Rationale:

ACLs can provide permissions beyond those permitted through the file mode and must be verified by file integrity tools.

Audit:

Verify that the SUSE operating system file integrity tool is configured to verify extended attributes.

If there is no application installed to perform integrity checks, this is a finding.

Check the "/etc/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 "acl" 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 "acl" rule is not being used on all 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 SUSE operating system file integrity tool to check file and directory ACLs.

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

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

1.171 SLES-15-040050 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The SUSE operating system file integrity tool must be configured to verify extended attributes.

```
GROUP ID: V-234987
RULE ID: SV-234987r991589
```

Rationale:

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

Audit:

Verify that the SUSE operating system file integrity tool is configured to verify extended attributes.

If there is no application installed to perform integrity checks, this is a finding.

Check the "/etc/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 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 SUSE operating system file integrity tool to check file and directory extended attributes.

If AIDE is installed, ensure the "xattrs" rule is present on all 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

1.172 SLES-15-040060 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The SUSE operating system must disable the x86 Ctrl-Alt-Delete key sequence.

```
GROUP ID: V-234988
RULE ID: SV-234988r991589
```

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 user interface 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 SUSE operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed.

Check that the ctrl-alt-del.target is masked with the following command:

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

If the ctrl-alt-del.target is not masked, 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
```

And reload the daemon to take effect

```
sudo systemctl daemon-reload
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.173 SLES-15-040061 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The SUSE operating system must disable the x86 Ctrl-Alt-Delete key sequence for Graphical User Interfaces.

```
GROUP ID: V-234989
RULE ID: SV-234989r991589
```

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 user interface 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 a graphical user interface is not installed, this requirement is Not Applicable.

Verify the SUSE operating system is not configured to reboot the system

when Ctrl-Alt-Delete is pressed in the graphical user interface.

Check that the dconf setting was disabled to allow the Ctrl-Alt-Delete

sequence in the graphical user interface with the following command:

Check the default logout key sequence:

```
sudo gsettings get org.gnome.settings-daemon.plugins.media-keys logout

['']
```

Check that the value is not writable and cannot be changed by the user:

```
sudo gsettings writable org.gnome.settings-daemon.plugins.media-keys logout

false
```

If the logout value is not [''] and the writable status is not false, this

is a finding.

Remediation:

Configure the system to disable the Ctrl-Alt-Delete sequence for the graphical user interface.

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

1. Create a user profile and with the listed content:

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

2. Create the following directories:

```
sudo mkdir -p /etc/dconf/db/local.d/
sudo mkdir -p /etc/dconf/db/local.d/locks/
```

3. Add the following files with the listed content:

```
/etc/dconf/db/local.d/01-fips-settings
[org/gnome/settings-daemon/plugins/media-keys]
logout=['']

/etc/dconf/db/local.d/locks/01-fips-locks
/org/gnome/settings-daemon/plugins/media-keys/logout
```

4. Update the dconf database:

```
sudo 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

1.174 SLES-15-040062 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The SUSE operating system must disable the systemd Ctrl-Alt-Delete burst key sequence.

```
GROUP ID: V-234990
RULE ID: SV-234990r991589
```

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 user interface 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 SUSE operating system is not configured to reboot the system when Ctrl-Alt-Delete is pressed seven times within two seconds with the following command:

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

CtrlAltDelBurstAction=none
```

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

Remediation:

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

```
CtrlAltDelBurstAction=none
```

Reload the daemon for this change to take effect

```
sudo systemctl daemon-reload
```

Additional Information:

CCI-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

1.175 SLES-15-040070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All SUSE operating system local interactive users must have a home directory assigned in the /etc/passwd file.

```
GROUP ID: V-234991
RULE ID: SV-234991r991589
```

Rationale:

If local interactive users are not assigned a valid home directory, there is no place for the storage and control of files they should own.

Audit:

Verify SUSE operating system local interactive users on the system have a home directory assigned.

Check for missing local interactive user home directories with the following command:

```
sudo pwck -r

user 'smithj': directory '/home/smithj' does not exist
```

Ask the System Administrator (SA) if any users found without home directories are local interactive users. If the SA is unable to provide a response, check for users with a User Identifier (UID) of 1000 or greater with the following command:

```
awk -F: '($3>=1000)&&($1!="nobody"){print $1 ":" $3}' /etc/passwd
```

If any interactive users do not have a home directory assigned, this is a finding.

Remediation:

Assign home directories to all SUSE operating system local interactive users that currently do not have a home directory assigned.

Assign a home directory to users via the usermod command:

```
sudo usermod -d /home/smithj 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

1.176 SLES-15-040080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All SUSE operating system local interactive user home directories defined in the /etc/passwd file must exist.

```
GROUP ID: V-234992
RULE ID: SV-234992r991589
```

Rationale:

If a local interactive user has a home directory defined that does not exist, the user may be given access to the / directory as the current working directory upon logon. This could create a Denial of Service because the user would not be able to access their logon configuration files, and it may give them visibility to system files they normally would not be able to access.

Audit:

Verify the assigned home directory of all SUSE operating system local interactive users on the system 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, $6}' /etc/passwd

smithj /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.

Check that all referenced home directories exist with the following command:

```
sudo pwck -r

user 'smithj': directory '/home/smithj' does not exist
```

If any home directories referenced in "/etc/passwd" are returned as not defined, this is a finding.

Remediation:

Create home directories to all SUSE operating system 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".

```
sudo mkdir /home/smithj
sudo chown smithj /home/smithj
sudo chgrp users /home/smithj
sudo 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

1.177 SLES-15-040090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All SUSE operating system local interactive user home directories must have mode 0750 or less permissive.

```
GROUP ID: V-234993
RULE ID: SV-234993r991589
```

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 SUSE operating system 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 SUSE operating system local 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".

```
sudo 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

1.178 SLES-15-040100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All SUSE operating system local interactive user home directories must be group-owned by the home directory owner's primary group.

```
GROUP ID: V-234994
RULE ID: SV-234994r991589
```

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 SUSE operating system local interactive users is group-owned by that user's primary GID.

Check the home directory assignment for all non-privileged users on the system with the following command:

Note: This may miss local interactive users that have been assigned a privileged User Identifier (UID). Evidence of interactive use may be obtained from a number of log files containing system logon information. The returned directory "/home/smithj" is used as an example.

```
awk -F: '($3>=1000)&&($7 !~ /nologin/){print $4, $6}' /etc/passwd

250:/home/smithj
```

Check the user's primary group with the following command:

```
grep users /etc/group

users:x:250:smithj,jonesj,jacksons
```

If the user home directory referenced in "/etc/passwd" is not group-owned by that user's primary GID, this is a finding.

Remediation:

Change the group owner of a SUSE operating system 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.

```
sudo 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

1.179 SLES-15-040110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All SUSE operating system local initialization files must have mode 0740 or less permissive.

```
GROUP ID: V-234995
RULE ID: SV-234995r991589
```

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 SUSE operating system local initialization files have a mode of "0740" or less permissive.

Check the mode on all SUSE operating system local initialization files with the following command:

Note: The example will be for the user "smithj", who has a home directory of "/home/smithj".

```
sudo ls -al /home/smithj/.* | more

-rwxr-xr-x 1 smithj users 896 Mar 10 2011 .profile
-rwxr-xr-x 1 smithj users 497 Jan 6 2007 .login
-rwxr-xr-x 1 smithj users 886 Jan 6 2007 .something
```

If any local initialization files have a mode more permissive than "0740", this is a finding.

Remediation:

Set the mode of SUSE operating system 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".

```
sudo chmod 0740 /home/smithj/.<INIT_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

1.180 SLES-15-040120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All SUSE operating system local interactive user initialization files executable search paths must contain only paths that resolve to the users home directory.

```
GROUP ID: V-234996
RULE ID: SV-234996r991589
```

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 SUSE operating system local interactive user initialization files executable search path statements do not contain statements that will reference a working directory other than the user's home directory.

Check the executable search path statement for all operating system local interactive user initialization files in the user's home directory with the following commands:

Note: The example will be for the user "smithj", who has a home directory of "/home/smithj".

```
sudo 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, and the additional path statements are not documented with the ISSO as an operational requirement, this is a finding.

Remediation:

Edit the SUSE operating system local interactive user initialization files to change any PATH variable statements for executables 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

1.181 SLES-15-040130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All SUSE operating system local initialization files must not execute world-writable programs.

```
GROUP ID: V-234997
RULE ID: SV-234997r991589
```

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 SUSE operating system local initialization files do not execute world-writable programs.

Verify that SUSE operating system local initialization files do not

execute world-writable programs.

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

```
sudo find / -xdev -perm -002 -type f -exec ls -ld {} \;
```

For all files listed, check for their presence in the local

initialization files with the following command:

Note: The example will be for a system that is configured to create

users' home directories in the "/home" directory.

```
sudo find /home/* -maxdepth 1 -type f -name \.\* -exec grep -H <file> {} \;
```

If any local initialization files are found to reference world-writable

files, this is a finding.

Remediation:

Remove the references to these files in the local initialization scripts or remove the world-writable permission of files referenced by SUSE operating system local initialization scripts with the following command:

```
sudo chmod 0755 <file>
```

Additional Information:

CCI-000366 Implement the security configuration settings.

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

1.182 SLES-15-040140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

SUSE operating system file systems that contain user home directories must be mounted to prevent files with the setuid and setgid bit set from being executed.

```
GROUP ID: V-234998
RULE ID: SV-234998r991589
```

Rationale:

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

Audit:

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

Print the currently active file system mount options of the file system(s) that contain the user home directories with the following command:

```
for X in `awk -F: '($3>=1000)&&($7 !~ /nologin/){print $6}' /etc/passwd`; do
findmnt -nkT $X; done | sort -r
/home /dev/mapper/system-home ext4 rw,nosuid,relatime,data=ordered
```

If a file system containing user home directories is not mounted with the FSTYPE OPTION nosuid, this is a finding.

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.

Remediation:

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

Re-mount the filesystems.

```
sudo mount -o remount /home
```

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

1.183 SLES-15-040150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

SUSE operating system file systems that are used with removable media must be mounted to prevent files with the setuid and setgid bit set from being executed.

```
GROUP ID: V-234999
RULE ID: SV-234999r991589
```

Rationale:

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

Audit:

Verify SUSE operating system file systems used for removable media are mounted with the "nosuid" option.

Check the file systems that are 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 SUSE operating system "/etc/fstab" file 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

1.184 SLES-15-040160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

SUSE operating system file systems that are being imported via Network File System (NFS) must be mounted to prevent files with the setuid and setgid bit set from being executed.

```
GROUP ID: V-235000
RULE ID: SV-235000r991589
```

Rationale:

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

Audit:

Verify SUSE operating system file systems that are being NFS exported are mounted with the "nosuid" option.

Find the file system(s) that contain the directories being exported with the following command:

```
grep nfs /etc/fstab

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.

Remediation:

Configure the SUSE operating system "/etc/fstab" file to use the "nosuid" option on file systems that are being exported 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

1.185 SLES-15-040170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

SUSE operating system file systems that are being imported via Network File System (NFS) must be mounted to prevent binary files from being executed.

```
GROUP ID: V-235001
RULE ID: SV-235001r991589
```

Rationale:

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

Audit:

Verify the SUSE operating system file systems that are being NFS exported are mounted with the "noexec" option.

Find the file system(s) that contain the directories being exported with the following command:

```
grep nfs /etc/fstab

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 exported binaries is not documented with the Information System Security Officer (ISSO) as an operational requirement, this is a finding.

Remediation:

Configure the SUSE operating system "/etc/fstab" file to use the "noexec" option on file systems that are being exported 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

1.186 SLES-15-040180 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All SUSE operating system world-writable directories must be group-owned by root, sys, bin, or an application group.

```
GROUP ID: V-235002
RULE ID: SV-235002r991589
```

Rationale:

If a world-writable directory has the sticky bit set and is not group-owned by a privileged Group Identifier (GID), unauthorized users may be able to modify files created by others.

The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage, (e.g., /tmp), and for directories requiring global read/write access.

Audit:

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

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

```
sudo find / -perm -002 -type d -exec ls -lLd {} \;

drwxrwxrwt. 2 root root 40 Aug 26 13:07 /dev/mqueue
drwxrwxrwt. 2 root root 220 Aug 26 13:23 /dev/shm
drwxrwxrwt. 14 root root 4096 Aug 26 13:29 /tmp
```

If any world-writable directories are not owned by root, sys, bin, or an application group associated with the directory, this is a finding.

Remediation:

Change the group of the SUSE operating system world-writable directories to root with the following command:

```
sudo chgrp root <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

1.187 SLES-15-040190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

SUSE operating system kernel core dumps must be disabled unless needed.

```
GROUP ID: V-235003
RULE ID: SV-235003r991589
```

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 SUSE operating system kernel core dumps are disabled unless needed.

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

```
systemctl status kdump.service
Loaded: not-found (Reason: No such file or directory)
Active: inactive (dead)
```

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 SUSE operating system kernel core dumps are not required, disable the "kdump" service with the following command:

```
sudo 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

1.188 SLES-15-040200 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

A separate file system must be used for SUSE operating system user home directories (such as /home or an equivalent).

```
GROUP ID: V-235004
RULE ID: SV-235004r991589
```

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 SUSE operating system non-privileged local interactive user home directories.

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

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

adamsj 1002 /home/adamsj /bin/bash
jacksonm 1003 /home/jacksonm /bin/bash
smithj 1001 /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 user's 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:

Create a separate file system/partition for SUSE operating system non-privileged local interactive user home directories.

Migrate the non-privileged local interactive user home directories onto the 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

1.189 SLES-15-040210 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The SUSE operating system must use a separate file system for /var.

```
GROUP ID: V-235005
RULE ID: SV-235005r991589
```

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 the SUSE operating system has a separate file system/partition 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:

Create a separate file system/partition on the SUSE operating system for "/var".

Migrate "/var" onto the 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

1.190 SLES-15-040220 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must be configured to not overwrite Pluggable Authentication Modules (PAM) configuration on package changes.

```
GROUP ID: V-235006
RULE ID: SV-235006r991589
```

Rationale:

The "pam-config" command line utility automatically generates a system PAM configuration as packages are installed, updated, or removed from the system. "pam-config" removes configurations for PAM modules and parameters that it does not know about. It may render ineffective PAM configuration by the system administrator and thus impact system security.

Audit:

Verify the SUSE operating system is configured to not overwrite PAM configuration on package changes.

Check that soft links between PAM configuration files are removed with the following command:

```
find /etc/pam.d/ -type l -iname "common-*"
```

If any results are returned, this is a finding.

Remediation:

Copy the PAM configuration files to their static locations and remove the SUSE operating system soft links for the PAM configuration files with the following command:

```
sudo sh -c 'for X in /etc/pam.d/common-*-pc; do cp -ivp --remove-destination
$X ${X:0:-3}; done'
```

Additional information on the configuration of multifactor authentication on the SUSE operating system can be found at https://www.suse.com/communities/blog/configuring-smart-card-authentication-suse-linux-enterprise/.

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

1.191 SLES-15-040230 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system SSH daemon must be configured to not allow authentication using known hosts authentication.

```
GROUP ID: V-235007
RULE ID: SV-235007r991589
```

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 SUSE operating system SSH daemon is configured to not allow authentication using "known hosts" authentication.

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

```
sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' | tr
'\n' ' ' | xargs sudo grep -iH '^\s*ignoreuserknownhosts'

IgnoreUserKnownHosts yes
```

If the value is returned as "no", the returned line is commented out, or no output is returned, this is a finding.

Remediation:

Configure the SUSE operating system 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
```

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

1.192 SLES-15-040240 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system SSH daemon public host key files must have mode 0644 or less permissive.

```
GROUP ID: V-235008
RULE ID: SV-235008r991589
```

Rationale:

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

Audit:

Verify the SUSE operating system SSH daemon 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 'ssh_host*key.pub' -exec stat -c "%a %n" {} \;

644 /etc/ssh/ssh_host_rsa_key.pub
644 /etc/ssh/ssh_host_dsa_key.pub
644 /etc/ssh/ssh_host_ecdsa_key.pub
644 /etc/ssh/ssh_host_ed25519_key.pub
```

If any file has a mode more permissive than "0644", this is a finding.

Remediation:

Configure the SUSE operating system SSH daemon 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.

Change the mode of public host key files under "/etc/ssh" to "0644" with the following command:

```
sudo chmod 0644 /etc/ssh/ssh_host*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

1.193 SLES-15-040250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system SSH daemon private host key files must have mode 0640 or less permissive.

```
GROUP ID: V-235009
RULE ID: SV-235009r991589
```

Rationale:

If an unauthorized user obtains the private SSH host key file, the host could be impersonated.

Audit:

Verify the SUSE operating system SSH daemon private host key files have mode "0640" or less permissive.

The following command will find all SSH private key files on the system:

```
sudo find / -name '*ssh_host*key' -exec ls -lL {} \;
```

Check the mode of the private host key files under "/etc/ssh" file with the following command:

```
find /etc/ssh -name 'ssh_host*key' -exec stat -c "%a %n" {} \;

640 /etc/ssh/ssh_host_rsa_key
640 /etc/ssh/ssh_host_dsa_key
640 /etc/ssh/ssh_host_ecdsa_key
640 /etc/ssh/ssh_host_ed25519_key
```

If any file has a mode more permissive than "0640", this is a finding.

Remediation:

Configure the mode of the SUSE operating system SSH daemon private host key files under "/etc/ssh" to "0640" with the following command:

```
sudo chmod 0640 /etc/ssh/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

1.194 SLES-15-040260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system SSH daemon must perform strict mode checking of home directory configuration files.

```
GROUP ID: V-235010
RULE ID: SV-235010r991589
```

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 SUSE operating system SSH daemon performs strict mode checking of home directory configuration files.

Check that the SSH daemon performs strict mode checking of home directory configuration files with the following command:

```
sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' | tr
'\n' ' ' | xargs sudo grep -iH '^\s*strictmodes'

StrictModes yes
```

If "StrictModes" is set to "no", is missing, or the returned line is commented out, this is a finding.

Remediation:

Configure the SUSE operating system SSH daemon performs strict mode checking of home directory configuration files.

Uncomment the "StrictModes" keyword in "/etc/ssh/sshd_config" and set the value to "yes":

```
StrictModes 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

1.195 SLES-15-040290 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system SSH daemon must disable forwarded remote X connections for interactive users, unless to fulfill documented and validated mission requirements.

```
GROUP ID: V-235013
RULE ID: SV-235013r991589
```

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.

Verify the SUSE operating system SSH daemon remote X forwarded connections for interactive users are disabled.

Check that SSH remote X forwarded connections are disabled with the following command:

```
sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' | tr
'\n' ' ' | xargs sudo grep -iH '^\s*x11forwarding'

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, is missing, or is commented out, this is a finding.

Remediation:

Configure the SUSE operating system SSH daemon to disable forwarded X connections for interactive users.

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
```

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 SLES-15-040300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must not forward Internet Protocol version 4 (IPv4) source-routed packets.

```
GROUP ID: V-235014
RULE ID: SV-235014r991589
```

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/IPv6 forwarding is enabled and the system is functioning as a router.

Audit:

Verify the SUSE operating system does not accept IPv4 source-routed packets.

Check the value of the IPv4 accept source route variable with the following command:

```
sudo sysctl net.ipv4.conf.all.accept_source_route

net.ipv4.conf.all.accept_source_route = 0
```

If the network parameter "ipv4.conf.all.accept_source_route" is not equal to "0" or nothing is returned, this is a finding.

Remediation:

Configure the SUSE operating system to disable IPv4 source routing by running the following command as an administrator:

```
sudo sysctl -w net.ipv4.conf.all.accept_source_route=0
```

If "0" is not the system's default value, add or update the following line in "/etc/sysctl.d/99-stig.conf":

```
sudo sh -c 'echo "net.ipv4.conf.all.accept_source_route=0" >>
/etc/sysctl.d/99-stig.conf'
sudo 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

1.197 SLES-15-040310 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must not forward Internet Protocol version 6 (IPv6) source-routed packets.

```
GROUP ID: V-235015
RULE ID: SV-235015r991589
```

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 SUSE operating system does not accept IPv6 source-routed packets.

Check the value of the IPv6 accept source route variable with the following command:

```
sudo sysctl net.ipv6.conf.all.accept_source_route

net.ipv6.conf.all.accept_source_route = 0
```

If the network parameter "ipv6.conf.all.accept_source_route" is not equal to "0" or nothing is returned, this is a finding.

Remediation:

Configure the SUSE operating system to disable IPv6 source routing by running the following command as an administrator:

```
sudo sysctl -w net.ipv6.conf.all.accept_source_route=0
```

If "0" is not the system's default value, add or update the following line in "/etc/sysctl.d/99-stig.conf":

```
sudo sh -c 'echo "net.ipv6.conf.all.accept_source_route=0" >>
/etc/sysctl.d/99-stig.conf'
sudo 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

1.198 SLES-15-040320 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must not forward Internet Protocol version 4 (IPv4) source-routed packets by default.

```
GROUP ID: V-235016
RULE ID: SV-235016r991589
```

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 SUSE operating system does not accept IPv4 source-routed packets by default.

Check the value of the default IPv4 accept source route variable with the following command:

```
sudo sysctl net.ipv4.conf.default.accept_source_route

net.ipv4.conf.default.accept_source_route = 0
```

If the network parameter "ipv4.conf.default.accept_source_route" is not equal to "0" or nothing is returned, this is a finding.

Remediation:

Configure the SUSE operating system to disable IPv4 default source routing by running the following command as an administrator:

```
sudo sysctl -w net.ipv4.conf.default.accept_source_route=0
```

If "0" is not the system's default value, add or update the following line in "/etc/sysctl.d/99-stig.conf":

```
sudo sh -c 'echo "net.ipv4.conf.default.accept_source_route=0" >>
/etc/sysctl.d/99-stig.conf'
sudo 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

1.199 SLES-15-040321 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must not forward Internet Protocol version 6 (IPv6) source-routed packets by default.

```
GROUP ID: V-235017
RULE ID: SV-235017r991589
```

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 SUSE operating system does not accept IPv6 source-routed packets by default.

Check the value of the default IPv6 accept source route variable with the following command:

```
sudo sysctl net.ipv6.conf.default.accept_source_route

net.ipv6.conf.default.accept_source_route = 0
```

If the network parameter "ipv6.conf.default.accept_source_route" is not equal to "0" or nothing is returned, this is a finding.

Remediation:

Configure the SUSE operating system to disable IPv6 default source routing by running the following command as an administrator:

```
sudo sysctl -w net.ipv6.conf.default.accept_source_route=0
```

If "0" is not the system's default value, add or update the following line in "/etc/sysctl.d/99-stig.conf":

```
sudo sh -c 'echo "net.ipv6.conf.default.accept_source_route=0" >>
/etc/sysctl.d/99-stig.conf'
sudo 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

1.200 SLES-15-040330 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must prevent Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages from being accepted.

```
GROUP ID: V-235018
RULE ID: SV-235018r991589
```

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 SUSE operating system does not accept IPv4 ICMP redirect messages.

Check the value of the IPv4 accept_redirects variable with the following command:

```
sudo sysctl net.ipv4.conf.all.accept_redirects

net.ipv4.conf.all.accept_redirects =0
```

If the network parameter "ipv4.conf.all.accept_redirects" is not equal to "0" or nothing is returned, this is a finding.

Remediation:

Configure the SUSE operating system to not accept IPv4 ICMP redirect messages by running the following command as an administrator:

```
sudo sysctl -w net.ipv4.conf.all.accept_redirects=0
```

If "0" is not the system's default value, add or update the following line in "/etc/sysctl.d/99-stig.conf":

```
sudo sh -c 'echo "net.ipv4.conf.all.accept_redirects=0" >> /etc/sysctl.d/99-
stig.conf'
sudo 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

1.201 SLES-15-040340 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must not allow interfaces to accept Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages by default.

```
GROUP ID: V-235019
RULE ID: SV-235019r991589
```

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 SUSE operating system does not accept IPv4 ICMP redirect messages by default.

Check the value of the default IPv4 accept_redirects variable with the following command:

```
sudo sysctl net.ipv4.conf.default.accept_redirects

net.ipv4.conf.default.accept_redirects = 0
```

If the network parameter "ipv4.conf.default.accept_redirects" is not equal to "0" or nothing is returned, this is a finding.

Remediation:

Configure the SUSE operating system to not accept IPv4 ICMP redirect messages by default by running the following command as an administrator:

```
sudo sysctl -w net.ipv4.conf.default.accept_redirects=0
```

If "0" is not the system's default value, add or update the following line in "/etc/sysctl.d/99-stig.conf":

```
sudo sh -c 'echo "net.ipv4.conf.default.accept_redirects=0" >>
/etc/sysctl.d/99-stig.conf'
sudo 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

1.202 SLES-15-040341 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must prevent Internet Protocol version 6 (IPv6) Internet Control Message Protocol (ICMP) redirect messages from being accepted.

```
GROUP ID: V-235020
RULE ID: SV-235020r991589
```

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 SUSE operating system does not accept IPv6 ICMP redirect messages.

Check the value of the IPv6 accept_redirects variable with the following command:

```
sudo sysctl net.ipv6.conf.all.accept_redirects

net.ipv6.conf.all.accept_redirects =0
```

If the network parameter "ipv6.conf.all.accept_redirects" is not equal to "0" or nothing is returned, this is a finding.

Remediation:

Configure the SUSE operating system to not accept IPv6 ICMP redirect messages by running the following command as an administrator:

```
sudo sysctl -w net.ipv6.conf.all.accept_redirects=0
```

If "0" is not the system's default value, add or update the following line in "/etc/sysctl.d/99-stig.conf":

```
sudo sh -c 'echo "net.ipv6.conf.all.accept_redirects=0" >> /etc/sysctl.d/99-
stig.conf'
sudo 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

1.203 SLES-15-040350 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must not allow interfaces to accept Internet Protocol version 6 (IPv6) Internet Control Message Protocol (ICMP) redirect messages by default.

```
GROUP ID: V-235021
RULE ID: SV-235021r991589
```

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 SUSE operating system does not allow IPv6 ICMP redirect messages by default.

Check the value of the default IPv6 accept_redirects variable with the following command:

```
sudo sysctl net.ipv6.conf.default.accept_redirects

net.ipv6.conf.default.accept_redirects = 0
```

If the network parameter "ipv6.conf.default.accept_redirects" is not equal to "0" or nothing is returned, this is a finding.

Remediation:

Configure the SUSE operating system to not accept IPv6 ICMP redirect messages by default by running the following command as an administrator:

```
sudo sysctl -w net.ipv6.conf.default.accept_redirects=0
```

If "0" is not the system's default value, add or update the following line in "/etc/sysctl.d/99-stig.conf":

```
sudo sh -c 'echo "net.ipv6.conf.default.accept_redirects=0" >>
/etc/sysctl.d/99-stig.conf'
sudo 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

1.204 SLES-15-040360 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must not allow interfaces to send Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirect messages by default.

```
GROUP ID: V-235022
RULE ID: SV-235022r991589
```

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 SUSE operating system does not allow interfaces to perform IPv4 ICMP redirects by default.

Check the value of the default IPv4 send_redirects variable with the following command:

```
sudo sysctl net.ipv4.conf.default.send_redirects

net.ipv4.conf.default.send_redirects = 0
```

If the network parameter "ipv4.conf.default.send_redirects" is not equal to "0" or nothing is returned, this is a finding.

Remediation:

Configure the SUSE operating system to not allow interfaces to perform IPv4 ICMP redirects by default by running the following command as an administrator:

```
sudo sysctl -w net.ipv4.conf.default.send_redirects=0
```

If "0" is not the system's default value, add or update the following line in "/etc/sysctl.d/99-stig.conf":

```
sudo sh -c 'echo "net.ipv4.conf.default.send_redirects=0" >>
/etc/sysctl.d/99-stig.conf'
sudo 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

1.205 SLES-15-040370 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must not send Internet Protocol version 4 (IPv4) Internet Control Message Protocol (ICMP) redirects.

```
GROUP ID: V-235023
RULE ID: SV-235023r991589
```

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 SUSE operating system does not allow interfaces to perform IPv4 ICMP redirects.

Check the value of the IPv4 send_redirects variable with the following command:

```
sudo sysctl net.ipv4.conf.all.send_redirects

net.ipv4.conf.all.send_redirects = 0
```

If the network parameter "ipv4.conf.all.send_redirects" is not equal to "0" or nothing is returned, this is a finding.

Remediation:

Configure the SUSE operating system to not allow interfaces to perform IPv4 ICMP redirects by running the following command as an administrator:

```
sudo sysctl -w net.ipv4.conf.all.send_redirects=0
```

If "0" is not the system's default value, add or update the following line in "/etc/sysctl.d/99-stig.conf":

```
sudo sh -c 'echo "net.ipv4.conf.all.send_redirects=0" >> /etc/sysctl.d/99-
stig.conf'
sudo 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

1.206 SLES-15-040380 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must not be performing Internet Protocol version 4 (IPv4) packet forwarding unless the system is a router.

```
GROUP ID: V-235024
RULE ID: SV-235024r991589
```

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 SUSE operating system is not performing IPv4 packet forwarding, unless the system is a router.

Check to see if IPv4 forwarding is disabled using the following command:

```
sudo sysctl net.ipv4.ip_forward

net.ipv4.ip_forward = 0
```

If the network parameter "ipv4.ip_forward" is not equal to "0" or nothing is returned, this is a finding.

Remediation:

Configure the SUSE operating system to not performing IPv4 packet forwarding by running the following command as an administrator:

```
sudo sysctl -w net.ipv4.ip_forward=0
```

If "0" is not the system's default value, add or update the following line in "/etc/sysctl.d/99-stig.conf":

```
sudo sh -c 'echo "net.ipv4.ip_forward=0" >> /etc/sysctl.d/99-stig.conf'
sudo 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

1.207 SLES-15-040381 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must not be performing Internet Protocol version 6 (IPv6) packet forwarding unless the system is a router.

```
GROUP ID: V-235025
RULE ID: SV-235025r991589
```

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 SUSE operating system is not performing IPv6 packet forwarding, unless the system is a router.

Check to see if IPv6 forwarding is enabled using the following command:

```
sudo sysctl net.ipv6.conf.all.forwarding

net.ipv6.conf.all.forwarding = 0
```

If the network parameter "ipv6.conf.all.forwarding" is not equal to "0" or nothing is returned, this is a finding.

Remediation:

Configure the SUSE operating system to not performing IPv6 packet forwarding by running the following command as an administrator:

```
sudo sysctl -w net.ipv6.conf.all.forwarding=0
```

If "0" is not the system's default value, add or update the following line in "/etc/sysctl.d/99-stig.conf":

```
sudo sh -c 'echo "net.ipv6.conf.all.forwarding=0" >> /etc/sysctl.d/99-
stig.conf'
sudo 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

1.208 SLES-15-040382 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must not be performing Internet Protocol version 6 (IPv6) packet forwarding by default unless the system is a router.

```
GROUP ID: V-235026
RULE ID: SV-235026r991589
```

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 SUSE operating system is not performing IPv6 packet forwarding by default, unless the system is a router.

Check to see if IPv6 forwarding is disabled by default using the following command:

```
sudo sysctl net.ipv6.conf.default.forwarding

net.ipv6.conf.default.forwarding = 0
```

If the network parameter "ipv6.conf.default.forwarding" is not equal to "0" or nothing is returned, this is a finding.

Remediation:

Configure the SUSE operating system to not performing IPv6 packet forwarding by default by running the following command as an administrator:

```
sudo sysctl -w net.ipv6.conf.default.forwarding=0
```

If "0" is not the system's default value, add or update the following line in "/etc/sysctl.d/99-stig.conf":

```
sudo sh -c 'echo "net.ipv6.conf.default.forwarding=0" >> /etc/sysctl.d/99-
stig.conf'
sudo 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

1.209 SLES-15-040390 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system must not have network interfaces in promiscuous mode unless approved and documented.

```
GROUP ID: V-235027
RULE ID: SV-235027r991589
```

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 then to collect information such as logon IDs, passwords, and key exchanges between systems.

If the system is being used to perform a network troubleshooting function, the use of these tools must be documented with the Information System Security Officer (ISSO) and restricted to only authorized personnel.

Audit:

Verify the SUSE operating system 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 the SUSE operating system network interfaces to turn off promiscuous mode unless approved by the ISSO and documented.

Set the promiscuous mode of an interface to off with the following command:

```
sudo ip link set dev <devicename> 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

1.210 SLES-15-040400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All SUSE operating system files and directories must have a valid owner.

```
GROUP ID: V-235028
RULE ID: SV-235028r991589
```

Rationale:

Unowned files and directories may be unintentionally inherited if a user is assigned the same User Identifier (UID) as the UID of the unowned files.

Audit:

Verify that all SUSE operating system 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.

```
sudo 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 SUSE operating 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:

```
sudo chown <user> <file>
```

Additional Information:

CCI-001230 Incorporate flaw remediation into the organizational configuration management process.

- NIST SP 800-53::SI-2 c
- NIST SP 800-53A::SI-2.1 (iv)
- NIST SP 800-53 Revision 4::SI-2 d
- NIST SP 800-53 Revision 5::SI-2 d

1.211 SLES-15-040410 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

All SUSE operating system files and directories must have a valid group owner.

```
GROUP ID: V-235029
RULE ID: SV-235029r991589
```

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 SUSE operating system 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.

```
sudo 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 SUSE operating 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:

```
sudo chgrp <group> <file>
```

Additional Information:

CCI-001230 Incorporate flaw remediation into the organizational configuration management process.

- NIST SP 800-53::SI-2 c
- NIST SP 800-53A::SI-2.1 (iv)
- NIST SP 800-53 Revision 4::SI-2 d
- NIST SP 800-53 Revision 5::SI-2 d

1.212 SLES-15-040420 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system default permissions must be defined in such a way that all authenticated users can only read and modify their own files.

```
GROUP ID: V-235030
RULE ID: SV-235030r991590
```

Rationale:

Setting the most restrictive default permissions ensures that when new accounts are created, they do not have unnecessary access.

Audit:

Verify the SUSE operating system defines default permissions for all authenticated users in such a way that the users can only read and modify their own files.

Check the system default permissions with the following command:

```
grep -i "^umask" /etc/login.defs

UMASK 077
```

If the "UMASK" variable is set to "000", the severity is raised to a CAT I, and this is a finding.

If the value of "UMASK" is not set to "077", or "UMASK" is missing, this is a finding.

Remediation:

Configure the SUSE operating system to define the default permissions for all authenticated users in such a way that the users can only read and modify their own files.

Add or edit the "UMASK" parameter in the "/etc/login.defs" file to match the example below:

```
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

1.213 SLES-15-040430 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The SUSE operating system must not allow unattended or automatic logon via the graphical user interface (GUI).

```
GROUP ID: V-235031
RULE ID: SV-235031r991591
```

Rationale:

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

Audit:

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

Verify the SUSE operating system does not allow unattended or automatic logon via the GUI.

Check that unattended or automatic login is disabled with the following commands:

```
grep -i ^DISPLAYMANAGER_AUTOLOGIN /etc/sysconfig/displaymanager

DISPLAYMANAGER_AUTOLOGIN=""
grep -i ^DISPLAYMANAGER_PASSWORD_LESS_LOGIN /etc/sysconfig/displaymanager

DISPLAYMANAGER_PASSWORD_LESS_LOGIN="no"
```

If the "DISPLAYMANAGER_AUTOLOGIN" parameter includes a username or the

```
"DISPLAYMANAGER_PASSWORD_LESS_LOGIN"
```

If parameter is not set to "no", this is a finding.

Remediation:

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

Configure the SUSE operating system GUI to not allow unattended or automatic logon to the system.

Add or edit the following lines in the "/etc/sysconfig/displaymanager"

configuration file:

```
DISPLAYMANAGER_AUTOLOGIN=""
DISPLAYMANAGER_PASSWORD_LESS_LOGIN="no"
```

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 SLES-15-040440 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The SUSE operating system must not allow unattended or automatic logon via SSH.

```
GROUP ID: V-235032
RULE ID: SV-235032r991591
```

Rationale:

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

Audit:

Verify the SUSE operating system disables unattended or automatic logon via SSH.

Check that unattended or automatic logon via SSH is disabled with the following command:

```
sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' | tr
'\n' ' ' | xargs sudo grep -iEH '^\s*(permit(.*?)(passwords|environment))'

PermitEmptyPasswords no
PermitUserEnvironment no
```

If "PermitEmptyPasswords" or "PermitUserEnvironment" keywords are not set to "no", are missing completely, or are commented out, this is a finding.

Remediation:

Configure the SUSE operating system disables unattended or automatic logon via SSH.

Add or edit the following lines in the "/etc/ssh/sshd_config" file:

```
PermitEmptyPasswords no
PermitUserEnvironment no
```

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 SLES-15-040450 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SUSE operating system SSH server must be configured to use only FIPS-validated key exchange algorithms.

```
GROUP ID: V-255920
RULE ID: SV-255920r991554
```

Rationale:

Without cryptographic integrity protections provided by FIPS-validated cryptographic algorithms, information can be viewed and altered by unauthorized users without detection.

The system will attempt to use the first algorithm presented by the client that matches the server list. Listing the values "strongest to weakest" is a method to ensure the use of the strongest algorithm available to secure the SSH connection.

Audit:

Verify the SSH server is configured to use only FIPS-validated key exchange algorithms:

```
sudo /usr/sbin/sshd -dd 2>&1 | awk '/filename/ {print $4}' | tr -d '\r' | tr
'\n' ' ' | xargs sudo grep -iH '^\s*kexalgorithms'

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)

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	SLES-15-010000 (Manual)	☐	☐
1.2	SLES-15-010010 (Manual)	☐	☐
1.3	SLES-15-010020 (Manual)	☐	☐
1.4	SLES-15-010030 (Manual)	☐	☐
1.5	SLES-15-010040 (Manual)	☐	☐
1.6	SLES-15-010050 (Manual)	☐	☐
1.7	SLES-15-010080 (Manual)	☐	☐
1.8	SLES-15-010090 (Manual)	☐	☐
1.9	SLES-15-010060 (Manual)	☐	☐
1.10	SLES-15-010100 (Manual)	☐	☐
1.11	SLES-15-010110 (Manual)	☐	☐
1.12	SLES-15-010120 (Manual)	☐	☐
1.13	SLES-15-010130 (Manual)	☐	☐
1.14	SLES-15-010140 (Manual)	☐	☐
1.15	SLES-15-010150 (Manual)	☐	☐
1.16	SLES-15-010160 (Manual)	☐	☐
1.17	SLES-15-010170 (Manual)	☐	☐
1.18	SLES-15-010180 (Manual)	☐	☐
1.19	SLES-15-010190 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	SLES-15-010200 (Manual)	☐	☐
1.21	SLES-15-010220 (Manual)	☐	☐
1.22	SLES-15-010230 (Manual)	☐	☐
1.23	SLES-15-010240 (Manual)	☐	☐
1.24	SLES-15-010260 (Manual)	☐	☐
1.25	SLES-15-010270 (Manual)	☐	☐
1.26	SLES-15-010280 (Manual)	☐	☐
1.27	SLES-15-010300 (Manual)	☐	☐
1.28	SLES-15-010310 (Manual)	☐	☐
1.29	SLES-15-010320 (Manual)	☐	☐
1.30	SLES-15-010330 (Manual)	☐	☐
1.31	SLES-15-010340 (Manual)	☐	☐
1.32	SLES-15-010350 (Manual)	☐	☐
1.33	SLES-15-010351 (Manual)	☐	☐
1.34	SLES-15-010352 (Manual)	☐	☐
1.35	SLES-15-010353 (Manual)	☐	☐
1.36	SLES-15-010354 (Manual)	☐	☐
1.37	SLES-15-010355 (Manual)	☐	☐
1.38	SLES-15-010356 (Manual)	☐	☐
1.39	SLES-15-010357 (Manual)	☐	☐
1.40	SLES-15-010358 (Manual)	☐	☐
1.41	SLES-15-010359 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	SLES-15-010360 (Manual)	☐	☐
1.43	SLES-15-010361 (Manual)	☐	☐
1.44	SLES-15-010362 (Manual)	☐	☐
1.45	SLES-15-010370 (Manual)	☐	☐
1.46	SLES-15-010375 (Manual)	☐	☐
1.47	SLES-15-010380 (Manual)	☐	☐
1.48	SLES-15-010390 (Manual)	☐	☐
1.49	SLES-15-010400 (Manual)	☐	☐
1.50	SLES-15-010410 (Manual)	☐	☐
1.51	SLES-15-010418 (Manual)	☐	☐
1.52	SLES-15-010419 (Manual)	☐	☐
1.53	SLES-15-010420 (Manual)	☐	☐
1.54	SLES-15-010430 (Manual)	☐	☐
1.55	SLES-15-010450 (Manual)	☐	☐
1.56	SLES-15-010460 (Manual)	☐	☐
1.57	SLES-15-010470 (Manual)	☐	☐
1.58	SLES-15-010480 (Manual)	☐	☐
1.59	SLES-15-010490 (Manual)	☐	☐
1.60	SLES-15-010500 (Manual)	☐	☐
1.61	SLES-15-010510 (Manual)	☐	☐
1.62	SLES-15-010530 (Manual)	☐	☐
1.63	SLES-15-010540 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	SLES-15-010550 (Manual)	☐	☐
1.65	SLES-15-010560 (Manual)	☐	☐
1.66	SLES-15-010570 (Manual)	☐	☐
1.67	SLES-15-010580 (Manual)	☐	☐
1.68	SLES-15-020000 (Manual)	☐	☐
1.69	SLES-15-020010 (Manual)	☐	☐
1.70	SLES-15-020020 (Manual)	☐	☐
1.71	SLES-15-020030 (Manual)	☐	☐
1.72	SLES-15-020040 (Manual)	☐	☐
1.73	SLES-15-020050 (Manual)	☐	☐
1.74	SLES-15-020060 (Manual)	☐	☐
1.75	SLES-15-020061 (Manual)	☐	☐
1.76	SLES-15-020080 (Manual)	☐	☐
1.77	SLES-15-020090 (Manual)	☐	☐
1.78	SLES-15-020091 (Manual)	☐	☐
1.79	SLES-15-020099 (Manual)	☐	☐
1.80	SLES-15-020100 (Manual)	☐	☐
1.81	SLES-15-020101 (Manual)	☐	☐
1.82	SLES-15-020102 (Manual)	☐	☐
1.83	SLES-15-020103 (Manual)	☐	☐
1.84	SLES-15-020104 (Manual)	☐	☐
1.85	SLES-15-020110 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.86	SLES-15-020120 (Manual)	☐	☐
1.87	SLES-15-020130 (Manual)	☐	☐
1.88	SLES-15-020140 (Manual)	☐	☐
1.89	SLES-15-020150 (Manual)	☐	☐
1.90	SLES-15-020160 (Manual)	☐	☐
1.91	SLES-15-020170 (Manual)	☐	☐
1.92	SLES-15-020180 (Manual)	☐	☐
1.93	SLES-15-020181 (Manual)	☐	☐
1.94	SLES-15-020190 (Manual)	☐	☐
1.95	SLES-15-020200 (Manual)	☐	☐
1.96	SLES-15-020210 (Manual)	☐	☐
1.97	SLES-15-020220 (Manual)	☐	☐
1.98	SLES-15-020230 (Manual)	☐	☐
1.99	SLES-15-020260 (Manual)	☐	☐
1.100	SLES-15-020270 (Manual)	☐	☐
1.101	SLES-15-020290 (Manual)	☐	☐
1.102	SLES-15-020300 (Manual)	☐	☐
1.103	SLES-15-030000 (Manual)	☐	☐
1.104	SLES-15-030010 (Manual)	☐	☐
1.105	SLES-15-030020 (Manual)	☐	☐
1.106	SLES-15-030030 (Manual)	☐	☐
1.107	SLES-15-030040 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.108	SLES-15-030050 (Manual)	☐	☐
1.109	SLES-15-030060 (Manual)	☐	☐
1.110	SLES-15-030070 (Manual)	☐	☐
1.111	SLES-15-030080 (Manual)	☐	☐
1.112	SLES-15-030090 (Manual)	☐	☐
1.113	SLES-15-030100 (Manual)	☐	☐
1.114	SLES-15-030110 (Manual)	☐	☐
1.115	SLES-15-030120 (Manual)	☐	☐
1.116	SLES-15-030130 (Manual)	☐	☐
1.117	SLES-15-030140 (Manual)	☐	☐
1.118	SLES-15-030150 (Manual)	☐	☐
1.119	SLES-15-030190 (Manual)	☐	☐
1.120	SLES-15-030250 (Manual)	☐	☐
1.121	SLES-15-030290 (Manual)	☐	☐
1.122	SLES-15-030330 (Manual)	☐	☐
1.123	SLES-15-030340 (Manual)	☐	☐
1.124	SLES-15-030350 (Manual)	☐	☐
1.125	SLES-15-030360 (Manual)	☐	☐
1.126	SLES-15-030370 (Manual)	☐	☐
1.127	SLES-15-030380 (Manual)	☐	☐
1.128	SLES-15-030390 (Manual)	☐	☐
1.129	SLES-15-030400 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.130	SLES-15-030410 (Manual)	☐	☐
1.131	SLES-15-030420 (Manual)	☐	☐
1.132	SLES-15-030430 (Manual)	☐	☐
1.133	SLES-15-030440 (Manual)	☐	☐
1.134	SLES-15-030450 (Manual)	☐	☐
1.135	SLES-15-030460 (Manual)	☐	☐
1.136	SLES-15-030470 (Manual)	☐	☐
1.137	SLES-15-030480 (Manual)	☐	☐
1.138	SLES-15-030490 (Manual)	☐	☐
1.139	SLES-15-030500 (Manual)	☐	☐
1.140	SLES-15-030510 (Manual)	☐	☐
1.141	SLES-15-030520 (Manual)	☐	☐
1.142	SLES-15-030530 (Manual)	☐	☐
1.143	SLES-15-030550 (Manual)	☐	☐
1.144	SLES-15-030560 (Manual)	☐	☐
1.145	SLES-15-030570 (Manual)	☐	☐
1.146	SLES-15-030580 (Manual)	☐	☐
1.147	SLES-15-030590 (Manual)	☐	☐
1.148	SLES-15-030600 (Manual)	☐	☐
1.149	SLES-15-030620 (Manual)	☐	☐
1.150	SLES-15-030630 (Manual)	☐	☐
1.151	SLES-15-030640 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.152	SLES-15-030650 (Manual)	☐	☐
1.153	SLES-15-030670 (Manual)	☐	☐
1.154	SLES-15-030680 (Manual)	☐	☐
1.155	SLES-15-030660 (Manual)	☐	☐
1.156	SLES-15-030690 (Manual)	☐	☐
1.157	SLES-15-030700 (Manual)	☐	☐
1.158	SLES-15-030760 (Manual)	☐	☐
1.159	SLES-15-030740 (Manual)	☐	☐
1.160	SLES-15-030770 (Manual)	☐	☐
1.161	SLES-15-030780 (Manual)	☐	☐
1.162	SLES-15-030790 (Manual)	☐	☐
1.163	SLES-15-030800 (Manual)	☐	☐
1.164	SLES-15-030810 (Manual)	☐	☐
1.165	SLES-15-030820 (Manual)	☐	☐
1.166	SLES-15-040000 (Manual)	☐	☐
1.167	SLES-15-040010 (Manual)	☐	☐
1.168	SLES-15-040020 (Manual)	☐	☐
1.169	SLES-15-040030 (Manual)	☐	☐
1.170	SLES-15-040040 (Manual)	☐	☐
1.171	SLES-15-040050 (Manual)	☐	☐
1.172	SLES-15-040060 (Manual)	☐	☐
1.173	SLES-15-040061 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.174	SLES-15-040062 (Manual)	☐	☐
1.175	SLES-15-040070 (Manual)	☐	☐
1.176	SLES-15-040080 (Manual)	☐	☐
1.177	SLES-15-040090 (Manual)	☐	☐
1.178	SLES-15-040100 (Manual)	☐	☐
1.179	SLES-15-040110 (Manual)	☐	☐
1.180	SLES-15-040120 (Manual)	☐	☐
1.181	SLES-15-040130 (Manual)	☐	☐
1.182	SLES-15-040140 (Manual)	☐	☐
1.183	SLES-15-040150 (Manual)	☐	☐
1.184	SLES-15-040160 (Manual)	☐	☐
1.185	SLES-15-040170 (Manual)	☐	☐
1.186	SLES-15-040180 (Manual)	☐	☐
1.187	SLES-15-040190 (Manual)	☐	☐
1.188	SLES-15-040200 (Manual)	☐	☐
1.189	SLES-15-040210 (Manual)	☐	☐
1.190	SLES-15-040220 (Manual)	☐	☐
1.191	SLES-15-040230 (Manual)	☐	☐
1.192	SLES-15-040240 (Manual)	☐	☐
1.193	SLES-15-040250 (Manual)	☐	☐
1.194	SLES-15-040260 (Manual)	☐	☐
1.195	SLES-15-040290 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.196	SLES-15-040300 (Manual)	☐	☐
1.197	SLES-15-040310 (Manual)	☐	☐
1.198	SLES-15-040320 (Manual)	☐	☐
1.199	SLES-15-040321 (Manual)	☐	☐
1.200	SLES-15-040330 (Manual)	☐	☐
1.201	SLES-15-040340 (Manual)	☐	☐
1.202	SLES-15-040341 (Manual)	☐	☐
1.203	SLES-15-040350 (Manual)	☐	☐
1.204	SLES-15-040360 (Manual)	☐	☐
1.205	SLES-15-040370 (Manual)	☐	☐
1.206	SLES-15-040380 (Manual)	☐	☐
1.207	SLES-15-040381 (Manual)	☐	☐
1.208	SLES-15-040382 (Manual)	☐	☐
1.209	SLES-15-040390 (Manual)	☐	☐
1.210	SLES-15-040400 (Manual)	☐	☐
1.211	SLES-15-040410 (Manual)	☐	☐
1.212	SLES-15-040420 (Manual)	☐	☐
1.213	SLES-15-040430 (Manual)	☐	☐
1.214	SLES-15-040440 (Manual)	☐	☐
1.215	SLES-15-040450 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 22, 2025	1.0.0	Initial CIS Release