# Tenable Vulnerability Management Report

Tenable Vulnerability Management

Sat, 03 May 2025 19:45:42 UTC

# Table Of Contents

# Audits FAILED

## 1.1.1.9 Ensure usb-storage kernel module is not available

### Info

USB storage provides a means to transfer and store files ensuring persistence and availability of the files independent of network connection status. Its popularity and utility has led to USB-based malware being a simple and common means for network infiltration and a first step to establishing a persistent threat within a networked environment.
Restricting USB access on the system will decrease the physical attack surface for a device and diminish the possible vectors to introduce malware.

### Solution

Run the following script to unload and disable the usb-storage module:
- IF - the usb-storage kernel module is available in ANY installed kernel:
- Create a file ending inconf with install usb-storage /bin/false in the /etc/modprobe.d/ directory
- Create a file ending inconf with blacklist usb-storage in the /etc/modprobe.d/ directory
- Run modprobe -r usb-storage 2>/dev/null; rmmod usb-storage 2>/dev/null to remove usb-storage from the kernel
- IF - the usb-storage kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

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

Impact:
Disabling the usb-storage module will disable any usage of USB storage devices.
If requirements and local site policy allow the use of such devices, other solutions should be configured accordingly instead. One example of a commonly used solution is USBGuard

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.8.7 |
| **800-171R3** | 03.08.07 |
| **800-53** | MP-7 |
| **800-53R5** | MP-7 |
| **CN-L3** | 8.5.4.1(c) |
| **CSCV7** | 13.7 |
| **CSCV8** | 10.3 |
| **CSF** | PR.PT-2 |

| | |
|---|---|
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.7.10 |
| **ISO/IEC-27001** | A.8.3.1 |
| **ISO/IEC-27001** | A.8.3.3 |
| **LEVEL** | 1A |
| **NESA** | T1.4.1 |

## Assets

### linux_project

```
The command script with multiple lines returned :

-- INFO --
 - module: "usb-storage" exists in:
  - "/usr/lib/modules/6.8.0-57-generic/kernel/drivers"
  - "/usr/lib/modules/6.8.0-58-generic/kernel/drivers"

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:
  - kernel module: "usb-storage" is loadable
  - kernel module: "usb-storage" is not deny listed
- Correctly set:
  - kernel module: "usb-storage" is not loaded
```

## 1.1.2.1.1 Ensure /tmp is a separate partition

### Info

The /tmp directory is a world-writable directory used for temporary storage by all users and some applications.
- IF - an entry for /tmp exists in /etc/fstab it will take precedence over entries in systemd default unit file.
Note: In an environment where the main system is diskless and connected to iSCSI, entries in /etc/fstab may not take precedence.
/tmp can be configured to use tmpfs
tmpfs puts everything into the kernel internal caches and grows and shrinks to accommodate the files it contains and is able to swap unneeded pages out to swap space. It has maximum size limits which can be adjusted on the fly via mount -o remount
Since tmpfs lives completely in the page cache and on swap, all tmpfs pages will be shown as "Shmem" in /proc/meminfo and "Shared" in free Notice that these counters also include shared memory. The most reliable way to get the count is using df and du
tmpfs has three mount options for sizing:
- size : The limit of allocated bytes for this tmpfs instance. The default is half of your physical RAM without swap. If you oversize your tmpfs instances the machine will deadlock since the OOM handler will not be able to free that memory.
- nr_blocks : The same as size, but in blocks of PAGE_SIZE.
- nr_inodes : The maximum number of inodes for this instance. The default is half of the number of your physical RAM pages, or (on a machine with highmem) the number of lowmem RAM pages, whichever is the lower.
These parameters accept a suffix k, m or g and can be changed on remount. The size parameter also accepts a suffix % to limit this tmpfs instance to that percentage of your physical RAM. The default, when neither size nor nr_blocks is specified, is size=50%
Making /tmp its own file system allows an administrator to set additional mount options such as the noexec option on the mount, making /tmp useless for an attacker to install executable code. It would also prevent an attacker from establishing a hard link to a system setuid program and wait for it to be updated. Once the program was updated, the hard link would be broken, and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.
This can be accomplished by either mounting tmpfs to /tmp or creating a separate partition for /tmp

### Solution

First ensure that systemd is correctly configured to ensure that /tmp will be mounted at boot time.
# systemctl unmask tmp.mount
For specific configuration requirements of the /tmp mount for your environment, modify /etc/fstab
Example of using tmpfs with specific mount options:
tmpfs /tmp tmpfs defaults,rw,nosuid,nodev,noexec,relatime,size=2G 0 0
Note: the size=2G is an example of setting a specific size for tmpfs
Example of using a volume or disk with specific mount options. The source location of the volume or disk will vary depending on your environment:
<device> /tmp <fstype> defaults,nodev,nosuid,noexec 0 0
Impact:
By design files saved to /tmp should have no expectation of surviving a reboot of the system. tmpfs is ram based and all files stored to tmpfs will be lost when the system is rebooted.
If files need to be persistent through a reboot, they should be saved to /var/tmp not /tmp
Since the /tmp directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to tmpfs or a separate partition.
Running out of /tmp space is a problem regardless of what kind of filesystem lies under it, but in a configuration where /tmp is not a separate file system it will essentially have the whole disk available, as the default installation only creates a single / partition. On the other hand, a RAM-based /tmp (as with tmpfs ) will almost certainly be much smaller, which can lead to applications filling up the filesystem much more easily. Another alternative is to create a dedicated partition for /tmp from a separate volume or disk. One of the downsides of a disk-based dedicated partition is that it will be slower than tmpfs which is RAM-based.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |

| | |
|---|---|
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command '/bin/findmnt -nk /tmp' did not return any result
```

## 1.1.2.2.4 Ensure noexec option set on /dev/shm partition

### Info

The noexec mount option specifies that the filesystem cannot contain executable binaries.
Setting this option on a file system prevents users from executing programs from shared memory. This deters users from introducing potentially malicious software on the system.

### Solution

- IF - a separate partition exists for /dev/shm
Edit the /etc/fstab file and add noexec to the fourth field (mounting options) for the /dev/shm partition.
Example:
tmpfs /dev/shm tmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0
Run the following command to remount /dev/shm with the configured options:
# mount -o remount /dev/shm
Note: It is recommended to use tmpfs as the device/filesystem type as /dev/shm is used as shared memory space by applications.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |

| | |
|---|---|
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |

| | |
|---|---|
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |

|  |  |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
Non-compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/dev/shm[\s]+' found - expect 'noexec' not found in the
 following lines:
          8: 31 26 0:26 / /dev/shm rw,nosuid,nodev shared:4 - tmpfs tmpfs rw,inode64
```

## 1.2.2.1 Ensure updates, patches, and additional security software are installed

### Info

Periodically patches are released for included software either due to security flaws or to include additional functionality.
Newer patches may contain security enhancements that would not be available through the latest full update. As a result, it is recommended that the latest software patches be used to take advantage of the latest functionality. As with any software installation, organizations need to determine if a given update meets their requirements and verify the compatibility and supportability of any additional software against the update revision that is selected.

### Solution

Run the following command to update all packages following local site policy guidance on applying updates and patches:

```
# apt update
# apt upgrade
- OR - # apt dist-upgrade
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.11.2 |
| **800-171** | 3.11.3 |
| **800-171** | 3.14.1 |
| **800-171R3** | 03.11.02 |
| **800-171R3** | 03.14.01 |
| **800-53** | RA-5 |
| **800-53** | SI-2 |
| **800-53** | SI-2(2) |
| **800-53R5** | RA-5 |
| **800-53R5** | RA-7 |
| **800-53R5** | SI-2 |
| **800-53R5** | SI-2(2) |
| **CN-L3** | 8.1.4.4(e) |
| **CN-L3** | 8.1.10.5(a) |
| **CN-L3** | 8.1.10.5(b) |
| **CN-L3** | 8.5.4.1(b) |
| **CN-L3** | 8.5.4.1(d) |
| **CN-L3** | 8.5.4.1(e) |
| **CSCV7** | 3.4 |
| **CSCV7** | 3.5 |
| **CSCV8** | 7.3 |

| | |
|---|---|
| **CSCV8** | 7.4 |
| **CSF** | DE.CM-8 |
| **CSF** | DE.DP-4 |
| **CSF** | DE.DP-5 |
| **CSF** | ID.RA-1 |
| **CSF** | PR.IP-12 |
| **CSF** | RS.CO-3 |
| **CSF** | RS.MI-3 |
| **CSF2.0** | GV.SC-10 |
| **CSF2.0** | ID.IM-01 |
| **CSF2.0** | ID.IM-02 |
| **CSF2.0** | ID.IM-03 |
| **CSF2.0** | ID.RA-01 |
| **CSF2.0** | ID.RA-08 |
| **CSF2.0** | PR.PS-02 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.6.8 |
| **ISO-27001-2022** | A.8.8 |
| **ISO-27001-2022** | A.8.32 |
| **ISO/IEC-27001** | A.12.6.1 |
| **ITSG-33** | RA-5 |
| **ITSG-33** | SI-2 |
| **ITSG-33** | SI-2(2) |
| **LEVEL** | 1M |
| **NESA** | M1.2.2 |
| **NESA** | M5.4.1 |
| **NESA** | T7.6.2 |
| **NESA** | T7.7.1 |
| **NIAV2** | PR9 |

| | |
|---|---|
| **PCI-DSSV3.2.1** | 6.1 |
| **PCI-DSSV3.2.1** | 6.2 |
| **PCI-DSSV4.0** | 6.3 |
| **PCI-DSSV4.0** | 6.3.1 |
| **PCI-DSSV4.0** | 6.3.3 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **SWIFT-CSCV1** | 2.2 |
| **SWIFT-CSCV1** | 2.7 |

## Assets

### linux_project

```
 The command '/bin/apt-get -s upgrade | /bin/grep -Ev '(Reading|Building|Calculating)''
 returned :

The following upgrades have been deferred due to phasing:
  grub-efi-amd64-bin grub-efi-amd64-signed
The following packages have been kept back:
  cloud-init linux-headers-generic linux-headers-virtual linux-image-virtual
  linux-virtual
The following packages will be upgraded:
  apparmor distro-info-data docker-buildx-plugin docker-ce docker-ce-cli
  docker-ce-rootless-extras docker-compose-plugin fwupd grub-common grub-pc
  grub-pc-bin grub2-common libapparmor1 libfwupd2 libnetplan1 linux-libc-dev
  linux-tools-common netplan-generator netplan.io python3-netplan
  ubuntu-pro-client ubuntu-pro-client-l10n
22 upgraded, 0 newly installed, 0 to remove and 7 not upgraded.
Inst distro-info-data [0.60ubuntu0.2] (0.60ubuntu0.3 Ubuntu:24.04/noble-updates [all])
Inst libapparmor1 [4.0.1really4.0.1-0ubuntu0.24.04.3] (4.0.1really4.0.1-0ubuntu0.24.04.4
 Ubuntu:24.04/noble-updates [amd64])
Inst netplan-generator [1.1.1-1~ubuntu24.04.1] (1.1.2-2~ubuntu24.04.1 Ubuntu:24.04/noble-updates
 [amd64]) []
Inst python3-netplan [1.1.1-1~ubuntu24.04.1] (1.1.2-2~ubuntu24.04.1 Ubuntu:24.04/noble-updates
 [amd64]) []
Inst netplan.io [1.1.1-1~ubuntu24.04.1] (1.1.2-2~ubuntu24.04.1 Ubuntu:24.04/noble-updates [amd64])
 []
Inst libnetplan1 [1.1.1-1~ubuntu24.04.1] (1.1.2-2~ubuntu24.04.1 Ubuntu:24.04/noble-updates
 [amd64])
Inst ubuntu-pro-client-l10n [34~24.04] (35.1ubuntu0~24.04 Ubuntu:24.04/noble-updates [amd64]) []
Inst ubuntu-pro-client [34~24.04] (35.1ubuntu0~24.04 Ubuntu:24.04/noble-updates [amd64])
Inst apparmor [4.0.1really4.0.1-0ubuntu0.24.04.3] (4.0.1really4.0.1-0ubuntu0.24.04.4 Ubuntu:24.04/
noble-updates [amd64])
Inst docker-buildx-plugin [0.22.0-1~ubuntu.24.04~noble] (0.23.0-1~ubuntu.24.04~noble Docker
 CE:noble [amd64])
Inst docker-ce-cli [5:28.0.4-1~ubuntu.24.04~noble] (5:28.1.1-1~ubuntu.24.04~noble Docker CE:noble
 [amd64])
Inst docker-ce [5:28.0.4-1~ubuntu.24.04~noble] (5:28.1.1-1~ubuntu.24.04~noble Docker CE:noble
 [...]
```

## 1.3.1.1 Ensure AppArmor is installed

### Info

AppArmor provides Mandatory Access Controls.
Without a Mandatory Access Control system installed only the default Discretionary Access Control system will be available.

### Solution

Install AppArmor.

```
# apt install apparmor apparmor-utils
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |

| | |
|---|---|
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |

| | |
|---|---|
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |

| | |
|---|---|
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - dpkg check apparmor-utils
The command '/bin/dpkg -s apparmor-utils 2>&1 | /bin/grep -E '(Status:|not installed)''
 returned :

dpkg-query: package 'apparmor-utils' is not installed and no information is available

-------------------------
PASSED - dpkg check apparmor
The command '/bin/dpkg -s apparmor 2>&1 | /bin/grep -E '(Status:|not installed)'' returned :

Status: install ok installed
```

## 1.3.1.2 Ensure AppArmor is enabled in the bootloader configuration

### Info

Configure AppArmor to be enabled at boot time and verify that it has not been overwritten by the bootloader boot parameters.
Note: This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.
AppArmor must be enabled at boot time in your bootloader configuration to ensure that the controls it provides are not overridden.

### Solution

Edit /etc/default/grub and add the apparmor=1 and security=apparmor parameters to the GRUB_CMDLINE_LINUX= line
GRUB_CMDLINE_LINUX="apparmor=1 security=apparmor"
Run the following command to update the grub2 configuration:
# update-grub

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |

| | |
|---|---|
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |

| | |
|---|---|
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |

|  |  |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
 All of the following must pass to satisfy this requirement:

-------------------------
FAILED - grub.cfg security=apparmor
Non-compliant file(s):
      /boot/grub/grub.cfg - regex '^[\s]*linux[\s]*' found - expect '(?i)security=apparmor(?-i)'
 not found in the following lines:
          159:  linux /vmlinuz-6.8.0-58-generic root=UUID=a191e346-9ec3-4394-b034-
b1545dbf4eaf ro console=tty0 console=ttyS0,115200 earlyprintk=ttyS0,115200 consoleblank=0
 memhp_default_state=online console=tty1 console=ttyS0
          178:   linux /vmlinuz-6.8.0-58-generic root=UUID=a191e346-9ec3-4394-b034-
b1545dbf4eaf ro console=tty0 console=ttyS0,115200 earlyprintk=ttyS0,115200 consoleblank=0
 memhp_default_state=online console=tty1 console=ttyS0
          196:   linux /vmlinuz-6.8.0-58-generic root=UUID=a191e346-9ec3-4394-b034-b1545dbf4eaf
 ro recovery nomodeset dis_ucode_ldr console=tty0 console=ttyS0,115200 earlyprintk=ttyS0,115200
 consoleblank=0 memhp_default_state=online
          215:   linux /vmlinuz-6.8.0-57-generic root=UUID=a191e346-9ec3-4394-b034-
b1545dbf4eaf ro console=tty0 console=ttyS0,115200 earlyprintk=ttyS0,115200 consoleblank=0
 memhp_default_state=online console=tty1 console=ttyS0
          233:   linux /vmlinuz-6.8.0-57-generic root=UUID=a191e346-9ec3-4394-b034-b1545dbf4eaf
 ro recovery nomodeset dis_ucode_ldr console=tty0 console=ttyS0,115200 earlyprintk=ttyS0,115200
 consoleblank=0 memhp_default_state=online

-------------------------
FAILED - grub.cfg apparmor=1
Non-compliant file(s):
      /boot/grub/grub.cfg - regex '^[\s]*linux[\s]*' found - expect '(?i)apparmor=1(?-i)' not
 found in the following lines:
          159:  linux /vmlinuz-6.8.0-58-generic root=UUID=a191e346-9ec3-4394-b034-
b1545dbf4eaf ro console=tty0 console=ttyS0,115200 earlyprintk=ttyS0,115200 consoleblank=0
 memhp_default_state=online console=tty1 console=ttyS0
          178:   linux /vmlinuz-6.8.0-58-generic root=UUID=a191e346-9ec3-4394-b034-b1545dbf4eaf ro
 console=tty0 console=ttyS0,115200 [...]
```

## 1.4.1 Ensure bootloader password is set

### Info

Setting the boot loader password will require that anyone rebooting the system must enter a password before being able to set command line boot parameters
Requiring a boot password upon execution of the boot loader will prevent an unauthorized user from entering boot parameters or changing the boot partition. This prevents users from weakening security (e.g. turning off AppArmor at boot time).

### Solution

Create an encrypted password with grub-mkpasswd-pbkdf2 :

```
# grub-mkpasswd-pbkdf2 --iteration-count=600000 --salt=64
Enter password: <password>
Reenter password: <password>
PBKDF2 hash of your password is <encrypted-password>
```

Add the following into a custom /etc/grub.d configuration file:

```
cat <<EOF exec tail -n +2 $0 set superusers="<username>"
password_pbkdf2 <username> <encrypted-password>
EOF
```

The superuser/user information and password should not be contained in the /etc/grub.d/00_header file as this file could be overwritten in a package update.
If there is a requirement to be able to boot/reboot without entering the password, edit /etc/grub.d/10_linux and add --unrestricted to the line CLASS=
Example:

```
CLASS="--class gnu-linux --class gnu --class os --unrestricted"
```

Run the following command to update the grub2 configuration:

```
# update-grub
```

Impact:
If password protection is enabled, only the designated superuser can edit a GRUB 2 menu item by pressing "e" or access the GRUB 2 command line by pressing "c"
If GRUB 2 is set up to boot automatically to a password-protected menu entry the user has no option to back out of the password prompt to select another menu entry. Holding the SHIFT key will not display the menu in this case. The user must enter the correct username and password. If unable to do so, the configuration files will have to be edited via a LiveCD or other means to fix the problem
You can add --unrestricted to the menu entries to allow the system to boot without entering a password. A password will still be required to edit menu items.
More Information:
https://help.ubuntu.com/community/Grub2/Passwords

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |

| | |
|---|---|
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |

| | |
|---|---|
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |

| | |
|---|---|
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - set superusers
The following file(s) do not contain "^[\s]*set[\s]*superusers[\s]*=":
      /boot/grub/grub.cfg

-------------------------
FAILED - password_pbkdf2
The following file(s) do not contain "^[\s]*password":
      /boot/grub/grub.cfg
```

## 1.5.1 Ensure address space layout randomization is enabled

### Info

Address space layout randomization (ASLR) is an exploit mitigation technique which randomly arranges the address space of key data areas of a process.
Randomly placing virtual memory regions will make it difficult to write memory page exploits as the memory placement will be consistently shifting.

### Solution

Set the following parameter in /etc/sysctl.conf or a file in /etc/sysctl.d/ ending inconf :
- kernel.randomize_va_space = 2
Example:
# printf "%s " "kernel.randomize_va_space = 2" >> /etc/sysctl.d/60-kernel_sysctl.conf
Run the following command to set the active kernel parameter:
# sysctl -w kernel.randomize_va_space=2
Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-53** | SI-16 |
| **800-53R5** | SI-16 |
| **CSCV7** | 8.3 |
| **CSCV8** | 10.5 |
| **CSF2.0** | PR.DS-10 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ITSG-33** | SI-16 |
| **LEVEL** | 1A |

### Assets

**linux_project**

```
The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:
 - "kernel.randomize_va_space" is not set in an included file
    ** Note: "kernel.randomize_va_space" May be set in a file that's ignored by load procedure **

- Correctly set:
 - "kernel.randomize_va_space" is correctly set to "2"
    in the running configuration
```

## 1.5.3 Ensure core dumps are restricted

### Info

A core dump is the memory of an executable program. It is generally used to determine why a program aborted. It can also be used to glean confidential information from a core file. The system provides the ability to set a soft limit for core dumps, but this can be overridden by the user.
Setting a hard limit on core dumps prevents users from overriding the soft variable. If core dumps are required, consider setting limits for user groups (see limits.conf(5) ). In addition, setting the fs.suid_dumpable variable to 0 will prevent setuid programs from dumping core.

### Solution

Add the following line to /etc/security/limits.conf or a /etc/security/limits.d/* file:
* hard core 0
Set the following parameter in /etc/sysctl.conf or a file in /etc/sysctl.d/ ending inconf :
- fs.suid_dumpable = 0
Example:
# printf "
%s" "fs.suid_dumpable = 0" >> /etc/sysctl.d/60-fs_sysctl.conf
Run the following command to set the active kernel parameter:
# sysctl -w fs.suid_dumpable=0
Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten
-IF- systemd-coredump is installed:
edit /etc/systemd/coredump.conf and add/modify the following lines:
Storage=none ProcessSizeMax=0
Run the command:
systemctl daemon-reload

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.7 |
| **800-171R3** | 03.01.07a. |
| **800-53** | AC-6(10) |
| **800-53R5** | AC-6(10) |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.10.6(a) |
| **CSF** | PR.AC-4 |
| **CSF2.0** | PR.AA-05 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.18 |

| | |
|---|---|
| **ITSG-33** | AC-6 |
| **LEVEL** | 1A |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - hard core 0
No matching files were found
Less than 1 matches of regex found

-------------------------
FAILED - fs.suid_dumpable
The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:
 - "fs.suid_dumpable" is incorrectly set to "2"
    in the running configuration
    and should have a value of: "0"
 - "fs.suid_dumpable" is not set in an included file
    ** Note: "fs.suid_dumpable" May be set in a file that's ignored by load procedure **
```

```
-------------------------
PASSED - check if systemd-coredump is installed
The command '/bin/systemctl list-unit-files | /bin/grep coredump | /bin/awk '{print} END {if (NR !
= 0) print "pass" ; else print "fail"}'' returned :

apport-coredump-hook@.service                                         static          -
pass
```

## 1.5.5 Ensure Automatic Error Reporting is not enabled

### Info

The Apport Error Reporting Service automatically generates crash reports for debugging
Apport collects potentially sensitive data, such as core dumps, stack traces, and log files. They can contain passwords, credit card numbers, serial numbers, and other private material.

### Solution

Edit /etc/default/apport and add or edit the enabled parameter to equal 0 :
enabled=0
Run the following commands to stop and mask the apport service
# systemctl stop apport.service # systemctl mask apport.service
- OR -
Run the following command to remove the apport package:
# apt purge apport

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |

|  |  |
|---|---|
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - check if apport.service is active
The command '/bin/systemctl is-active apport.service | /bin/grep '^active' | /bin/awk '{print} END
 {if(NR==0) print "pass"}'' returned :

active

-------------------------
FAILED - /etc/default/apport - enabled
Non-compliant file(s):
      /etc/default/apport - regex '^\h*enabled\h*=\h*[^0]\b$' found - expect '^\h*enabled\h*=
\h*[^0]\b$' found in the following lines:
          4: enabled=1
```

## 1.6.2 Ensure local login warning banner is configured properly

### Info

The contents of the /etc/issue file are displayed to users prior to login for local terminals.
Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If mingetty(8) supports the following options, they display operating system information: m - machine architecture r - operating system release s - operating system name v - operating system version - or the operating system's name
Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " uname -a " command once they have logged in.

### Solution

Edit the /etc/issue file with the appropriate contents according to your site policy, remove any instances of m r s v or references to the OS platform
Example:
# echo "Authorized users only. All activity may be monitored and reported." > /etc/issue

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.9 |
| **800-171R3** | 03.01.09 |
| **800-53** | AC-8 |
| **800-53R5** | AC-8 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.5 |
| **ITSG-33** | AC-8 |
| **LEVEL** | 1A |
| **NESA** | M1.3.6 |
| **TBA-FIISB** | 45.2.4 |

### Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - Banner content
First ERROR: Ubuntu 24.04.2 != All activities
Ubuntu 24.04.2 LTS \n \l

-------------------------
PASSED - mrsv not included in /etc/issue
The following file(s) do not contain "\\[mrsv]":
      /etc/issue
```

## 1.6.3 Ensure remote login warning banner is configured properly

### Info

The contents of the /etc/issue.net file are displayed to users prior to login for remote connections from configured services.
Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform.
If mingetty(8) supports the following options, they display operating system information: m - machine architecture r - operating system release s - operating system name v - operating system version
Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place.
Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " uname -a " command once they have logged in.

### Solution

Edit the /etc/issue.net file with the appropriate contents according to your site policy, remove any instances of m r s v or references to the OS platform
Example:
# echo "Authorized users only. All activity may be monitored and reported." > /etc/issue.net

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.9 |
| **800-171R3** | 03.01.09 |
| **800-53** | AC-8 |
| **800-53R5** | AC-8 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.5 |
| **ITSG-33** | AC-8 |
| **LEVEL** | 1A |
| **NESA** | M1.3.6 |
| **TBA-FIISB** | 45.2.4 |

### Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - mrsv not included in /etc/issue.net
The following file(s) do not contain "\\[mrsv]":
      /etc/issue.net

-------------------------
FAILED - banner text
First ERROR: Ubuntu 24.04.2 != All activities
Ubuntu 24.04.2 LTS
```

## 2.2.4 Ensure telnet client is not installed

### Info

The inetutils-telnet package contains the telnet client, which allows users to start connections to other systems via the telnet protocol.
The telnet protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow an unauthorized user to steal credentials. The ssh package provides an encrypted session and stronger security and is included in most Linux distributions.

### Solution

Run the following commands to uninstall telnet & inetutils-telnet :
# apt purge telnet # apt purge inetutils-telnet
Impact:
Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |

| | |
|---|---|
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - Ensure package name equals 'inetutils-telnet' is not installed
The command '/bin/dpkg -s inetutils-telnet 2>&1 | /bin/grep -E '(^Status:|not installed)''
 returned :

Status: install ok installed

-------------------------
FAILED - Ensure package name equals 'telnet' is not installed
The command '/bin/dpkg -s telnet 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

Status: install ok installed
```

## 2.2.6 Ensure ftp client is not installed

### Info

tnftp an enhanced FTP client, is the user interface to the Internet standard File Transfer Protocol. The program allows a user to transfer files to and from a remote network site.
Unless there is a need to run the system using Internet standard File Transfer Protocol (for example, to allow anonymous downloads), it is recommended that the package be removed to reduce the potential attack surface.

### Solution

Run the following commands to uninstall tnftp & ftp :
# apt purge ftp # apt purge tnftp

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |

| SWIFT-CSCV1 | 2.3 |
|---|---|

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - Ensure package name equals 'ftp' is not installed
The command '/bin/dpkg -s ftp 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

Status: install ok installed

-------------------------
FAILED - Ensure package name equals 'tnftp' is not installed
The command '/bin/dpkg -s tnftp 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

Status: install ok installed
```

## 2.3.2.1 Ensure systemd-timesyncd configured with authorized timeserver

### Info

NTP=
- A space-separated list of NTP server host names or IP addresses. During runtime this list is combined with any per-interface NTP servers acquired from systemd-networkd.service(8). systemd-timesyncd will contact all configured system or per-interface servers in turn, until one responds. When the empty string is assigned, the list of NTP servers is reset, and all prior assignments will have no effect. This setting defaults to an empty list.
FallbackNTP=
- A space-separated list of NTP server host names or IP addresses to be used as the fallback NTP servers. Any per-interface NTP servers obtained from systemd-networkd.service(8) take precedence over this setting, as do any servers set via NTP= above. This setting is hence only relevant if no other NTP server information is known. When the empty string is assigned, the list of NTP servers is reset, and all prior assignments will have no effect. If this option is not given, a compiled-in list of NTP servers is used.
Time synchronization is important to support time sensitive security mechanisms and to ensure log files have consistent time records across the enterprise to aid in forensic investigations

### Solution

Set NTP and/or FallbackNPT parameters to local site approved authoritative time server(s) in /etc/systemd/timesyncd.conf or a file in /etc/systemd/timesyncd.conf.d/ ending inconf in the [Time] section:
Example file:
[Time] NTP=time.nist.gov # Uses the generic name for NIST's time servers FallbackNTP=time-a-g.nist.gov time-b-g.nist.gov time-c-g.nist.gov # Space separated list of NIST time servers
Example script to create systemd drop-in configuration file:
#!/usr/bin/env bash
{ a_settings=("NTP=time.nist.gov" "FallbackNTP=time-a-g.nist.gov time-b-g.nist.gov time-c-g.nist.gov") [ ! -d /etc/systemd/timesyncd.conf.d/ ] && mkdir /etc/systemd/timesyncd.conf.d/ if grep -Psq -- '^h*[Time]' /etc/systemd/timesyncd.conf.d/60-timesyncd.conf; then printf '%s ' "" "${a_settings[@]}" >> /etc/systemd/timesyncd.conf.d/60-timesyncd.conf else printf '%s ' "" "[Time]" "${a_settings[@]}" >> /etc/systemd/timesyncd.conf.d/60-timesyncd.conf fi }
Note: If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten
Run to following command to update the parameters in the service:
# systemctl reload-or-restart systemd-journald

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.6 |
| **800-171** | 3.3.7 |
| **800-171R3** | 03.03.06a. |
| **800-171R3** | 03.03.07 |
| **800-53** | AU-7 |
| **800-53** | AU-8 |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-8 |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 8.1.4.3(b) |
| **CSCV7** | 6.1 |
| **CSCV8** | 8.4 |
| **CSF** | PR.PT-1 |

| | |
|---|---|
| **CSF** | RS.AN-3 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.8.17 |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-8 |
| **LEVEL** | 1A |
| **NESA** | T3.6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |
| **TBA-FIISB** | 37.4 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:
 - "NTP" is not set in an included file
   *** Note: "NTP" May be set in a file that's ignored by load procedure ***
 - "FallbackNTP" is not set in an included file
   *** Note: "FallbackNTP" May be set in a file that's ignored by load procedure ***
```

## 2.4.1.2 Ensure permissions on /etc/crontab are configured

### Info

The /etc/crontab file is used by cron to control its own jobs. The commands in this item make sure that root is the user and group owner of the file and that only the owner can access the file.
This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

### Solution

- IF - cron is installed on the system:
Run the following commands to set ownership and permissions on /etc/crontab :
# chown root:root /etc/crontab # chmod og-rwx /etc/crontab

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |

| | |
|---|---|
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |

| | |
|---|---|
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |

|  |  |
|---|---|
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The file /etc/crontab with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 177 uneven
 permissions : FALSE

/etc/crontab
```

## 2.4.1.3 Ensure permissions on /etc/cron.hourly are configured

### Info

This directory contains system cron jobs that need to run on an hourly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.
Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

### Solution

- IF - cron is installed on the system:
Run the following commands to set ownership and permissions on the /etc/cron.hourly directory:

```
# chown root:root /etc/cron.hourly/ # chmod og-rwx /etc/cron.hourly/
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |

| | |
|---|---|
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |

| | |
|---|---|
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |

| | |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The file /etc/cron.hourly with fmode owner: root group: root mode: 0755 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 077 uneven
 permissions : FALSE

/etc/cron.hourly
```

## 2.4.1.4 Ensure permissions on /etc/cron.daily are configured

### Info

The /etc/cron.daily directory contains system cron jobs that need to run on a daily basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.
Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

### Solution

- IF - cron is installed on the system:
Run the following commands to set ownership and permissions on the /etc/cron.daily directory:
# chown root:root /etc/cron.daily/ # chmod og-rwx /etc/cron.daily/

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |

| | |
|---|---|
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |

| | |
|---|---|
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |

| | |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The file /etc/cron.daily with fmode owner: root group: root mode: 0755 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 077 uneven
 permissions : FALSE

/etc/cron.daily
```

## 2.4.1.5 Ensure permissions on /etc/cron.weekly are configured

### Info

The /etc/cron.weekly directory contains system cron jobs that need to run on a weekly basis. The files in this directory cannot be manipulated by the crontab command but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.
Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

### Solution

- IF - cron is installed on the system:
Run the following commands to set ownership and permissions on the /etc/cron.weekly directory:
# chown root:root /etc/cron.weekly/ # chmod og-rwx /etc/cron.weekly/

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |

| | |
|---|---|
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |

| | |
|---|---|
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |

|  |  |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The file /etc/cron.weekly with fmode owner: root group: root mode: 0755 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 077 uneven
 permissions : FALSE

/etc/cron.weekly
```

## 2.4.1.6 Ensure permissions on /etc/cron.monthly are configured

### Info

The /etc/cron.monthly directory contains system cron jobs that need to run on a monthly basis. The files in this directory cannot be manipulated by the crontab command but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

### Solution

- IF - cron is installed on the system:

Run the following commands to set ownership and permissions on the /etc/cron.monthly directory:

# chown root:root /etc/cron.monthly/ # chmod og-rwx /etc/cron.monthly/

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |

| | |
|---|---|
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |

| | |
|---|---|
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |

| | |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The file /etc/cron.monthly with fmode owner: root group: root mode: 0755 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 077 uneven
 permissions : FALSE

/etc/cron.monthly
```

## 2.4.1.7 Ensure permissions on /etc/cron.d are configured

### Info

The /etc/cron.d directory contains system cron jobs that need to run in a similar manner to the hourly, daily weekly and monthly jobs from /etc/crontab but require more granular control as to when they run. The files in this directory cannot be manipulated by the crontab command but are instead edited by system administrators using a text editor.
The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.
Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

### Solution

- IF - cron is installed on the system:
Run the following commands to set ownership and permissions on the /etc/cron.d directory:
# chown root:root /etc/cron.d/ # chmod og-rwx /etc/cron.d/

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |

| | |
|---|---|
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |

| | |
|---|---|
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |

| | |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The file /etc/cron.d with fmode owner: root group: root mode: 0755 uid: 0 gid: 0 uneven
 permissions : FALSE  does not match the policy value owner: root group: root mask: 077 uneven
 permissions : FALSE

/etc/cron.d
```

## 2.4.1.8 Ensure crontab is restricted to authorized users

### Info

crontab is the program used to install, deinstall, or list the tables used to drive the cron daemon. Each user can have their own crontab, and though these are files in /var/spool/cron/crontabs they are not intended to be edited directly.
If the /etc/cron.allow file exists, then you must be listed (one user per line) therein in order to be allowed to use this command. If the /etc/cron.allow file does not exist but the /etc/cron.deny file does exist, then you must not be listed in the /etc/cron.deny file in order to use this command.
If neither of these files exists, then depending on site-dependent configuration parameters, only the super user will be allowed to use this command, or all users will be able to use this command.
If both files exist then /etc/cron.allow takes precedence. Which means that /etc/cron.deny is not considered and your user must be listed in /etc/cron.allow in order to be able to use the crontab.
Regardless of the existence of any of these files, the root administrative user is always allowed to setup a crontab.
The files /etc/cron.allow and /etc/cron.deny if they exist, must be either world-readable, or readable by group crontab If they are not, then cron will deny access to all users until the permissions are fixed.
There is one file for each user's crontab under the /var/spool/cron/crontabs directory. Users are not allowed to edit the files under that directory directly to ensure that only users allowed by the system to run periodic tasks can add them, and only syntactically correct crontabs will be written there. This is enforced by having the directory writable only by the crontab group and configuring crontab command with the setgid bid set for that specific group.
Note:
- Even though a given user is not listed in cron.allow cron jobs can still be run as that user
- The files /etc/cron.allow and /etc/cron.deny if they exist, only controls administrative access to the crontab command for scheduling and modifying cron jobs
On many systems, only the system administrator is authorized to schedule cron jobs. Using the cron.allow file to control who can run cron jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

### Solution

- IF - cron is installed on the system:
Run the following script to:
- Create /etc/cron.allow if it doesn't exist
- Change owner to user root
- Change group owner to group root - OR - group crontab if it exists
- Change mode to 640 or more restrictive

```
#!/usr/bin/env bash
{ [ ! -e "/etc/cron.deny" ] && touch /etc/cron.allow chmod u-x,g-wx,o-rwx /etc/cron.allow if grep -Pq -- '^h*crontab:' /etc/group; then chown root:crontab /etc/cron.allow else chown root:root /etc/cron.allow fi }
```

- IF - /etc/cron.deny exists, run the following script to:
- Change owner to user root
- Change group owner to group root - OR - group crontab if it exists
- Change mode to 640 or more restrictive

```
#!/usr/bin/env bash
{ if [ -e "/etc/cron.deny" ]; then chmod u-x,g-wx,o-rwx /etc/cron.deny if grep -Pq -- '^h*crontab:' /etc/group; then chown root:crontab /etc/cron.deny else chown root:root /etc/cron.deny fi fi }
```

Note: On systems where cron is configured to use the group crontab if the group crontab is not set as the owner of cron.allow then cron will deny access to all users and you will see an error similar to:
You (<USERNAME>) are not allowed to use this program (crontab) See crontab(1) for more information

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |

| | |
|---|---|
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |

| | |
|---|---|
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |

| | |
|---|---|
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - /etc/cron.allow file permissions
No files found: /etc/cron.allow

-------------------------
PASSED - /etc/cron.deny file permissions
```

## 3.3.1 Ensure ip forwarding is disabled

### Info

The net.ipv4.ip_forward and net.ipv6.conf.all.forwarding flags are used to tell the system whether it can forward packets or not.
Setting net.ipv4.ip_forward and net.ipv6.conf.all.forwarding to 0 ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

### Solution

Set the following parameter in /etc/sysctl.conf or a file in /etc/sysctl.d/ ending inconf :
- net.ipv4.ip_forward = 0

Example:

```
# printf '%s ' "net.ipv4.ip_forward = 0" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

```
#!/usr/bin/env bash
{ sysctl -w net.ipv4.ip_forward=0 sysctl -w net.ipv4.route.flush=1 }
```

- IF - IPv6 is enabled on the system:

Set the following parameter in /etc/sysctl.conf or a file in /etc/sysctl.d/ ending inconf :
- net.ipv6.conf.all.forwarding = 0

Example:

```
# printf '%s ' "net.ipv6.conf.all.forwarding = 0" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```

Run the following script to set the active kernel parameters:

```
#!/usr/bin/env bash
{ sysctl -w net.ipv6.conf.all.forwarding=0 sysctl -w net.ipv6.route.flush=1 }
```

Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten
Impact:
IP forwarding is required on systems configured to act as a router. If these parameters are disabled, the system will not be able to perform as a router.
Many Cloud Service Provider (CSP) hosted systems require IP forwarding to be enabled. If the system is running on a CSP platform, this requirement should be reviewed before disabling IP forwarding.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |

|  |  |
|---|---|
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:
 - "net.ipv4.ip_forward" is incorrectly set to "1"
    in the running configuration
    and should have a value of: "0"
 - "net.ipv4.ip_forward" is incorrectly set to "1"
    in "/etc/sysctl.conf"
    and should have a value of: "0"
 - "net.ipv6.conf.all.forwarding" is not set in an included file
    ** Note: "net.ipv6.conf.all.forwarding" May be set in a file that's ignored by load procedure
 **

- Correctly set:
 - "net.ipv6.conf.all.forwarding" is correctly set to "0"
    in the running configuration
```

## 3.3.10 Ensure tcp syn cookies is enabled

### Info

When tcp_syncookies is set, the kernel will handle TCP SYN packets normally until the half-open connection queue is full, at which time, the SYN cookie functionality kicks in. SYN cookies work by not using the SYN queue at all. Instead, the kernel simply replies to the SYN with a SYN/ACK, but will include a specially crafted TCP sequence number that encodes the source and destination IP address and port number and the time the packet was sent. A legitimate connection would send the ACK packet of the three way handshake with the specially crafted sequence number. This allows the system to verify that it has received a valid response to a SYN cookie and allow the connection, even though there is no corresponding SYN in the queue.

Attackers use SYN flood attacks to perform a denial of service attacked on a system by sending many SYN packets without completing the three way handshake. This will quickly use up slots in the kernel's half-open connection queue and prevent legitimate connections from succeeding. Setting net.ipv4.tcp_syncookies to 1 enables SYN cookies, allowing the system to keep accepting valid connections, even if under a denial of service attack.

### Solution

Set the following parameter in /etc/sysctl.conf or a file in /etc/sysctl.d/ ending inconf :

- net.ipv4.tcp_syncookies = 1

Example:

```
# printf '%s ' "net.ipv4.tcp_syncookies = 1" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

```
#!/usr/bin/env bash
{ sysctl -w net.ipv4.tcp_syncookies=1 sysctl -w net.ipv4.route.flush=1 }
```

Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |

| | |
|---|---|
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:
 - "net.ipv4.tcp_syncookies" is not set in an included file
    ** Note: "net.ipv4.tcp_syncookies" May be set in a file that's ignored by load procedure **

- Correctly set:
 - "net.ipv4.tcp_syncookies" is correctly set to "1"
    in the running configuration
```

## 3.3.11 Ensure ipv6 router advertisements are not accepted

### Info

Routers periodically multicast Router Advertisement messages to announce their availability and convey information to neighboring nodes that enable them to be automatically configured on the network.
net.ipv6.conf.all.accept_ra and net.ipv6.conf.default.accept_ra determine the systems ability to accept these advertisements
It is recommended that systems do not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes. Setting net.ipv6.conf.all.accept_ra and net.ipv6.conf.default.accept_ra to 0 disables the system's ability to accept IPv6 router advertisements.

### Solution

- IF - IPv6 is enabled on the system:
Set the following parameters in /etc/sysctl.conf or a file in /etc/sysctl.d/ ending inconf :
- net.ipv6.conf.all.accept_ra = 0
- net.ipv6.conf.default.accept_ra = 0
Example:
# printf '%s ' "net.ipv6.conf.all.accept_ra = 0" "net.ipv6.conf.default.accept_ra = 0" >> /etc/sysctl.d/60-netipv6_sysctl.conf
Run the following script to set the active kernel parameters:
#!/usr/bin/env bash
{ sysctl -w net.ipv6.conf.all.accept_ra=0 sysctl -w net.ipv6.conf.default.accept_ra=0 sysctl -w net.ipv6.route.flush=1 }
Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |

| | |
|---|---|
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:
 - "net.ipv6.conf.all.accept_ra" is incorrectly set to "1"
    in the running configuration
    and should have a value of: "0"
 - "net.ipv6.conf.all.accept_ra" is not set in an included file
    ** Note: "net.ipv6.conf.all.accept_ra" May be set in a file that's ignored by load procedure
 **
 - "net.ipv6.conf.default.accept_ra" is incorrectly set to "1"
    in the running configuration
    and should have a value of: "0"
 - "net.ipv6.conf.default.accept_ra" is not set in an included file
    ** Note: "net.ipv6.conf.default.accept_ra" May be set in a file that's ignored by load
 procedure **
```

## 3.3.2 Ensure packet redirect sending is disabled

### Info

ICMP Redirects are used to send routing information to other hosts. As a host itself does not act as a router (in a host only configuration), there is no need to send redirects.
An attacker could use a compromised host to send invalid ICMP redirects to other router devices in an attempt to corrupt routing and have users access a system set up by the attacker as opposed to a valid system.

### Solution

Set the following parameters in /etc/sysctl.conf or a file in /etc/sysctl.d/ ending inconf :
- net.ipv4.conf.all.send_redirects = 0
- net.ipv4.conf.default.send_redirects = 0
Example:
# printf '%s ' "net.ipv4.conf.all.send_redirects = 0" "net.ipv4.conf.default.send_redirects = 0" >> /etc/sysctl.d/60-netipv4_sysctl.conf
Run the following script to set the active kernel parameters:
#!/usr/bin/env bash
{ sysctl -w net.ipv4.conf.all.send_redirects=0 sysctl -w net.ipv4.conf.default.send_redirects=0 sysctl -w net.ipv4.route.flush=1 }
Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten
Impact:
IP forwarding is required on systems configured to act as a router. If these parameters are disabled, the system will not be able to perform as a router.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |

| | |
|---|---|
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:
 - "net.ipv4.conf.all.send_redirects" is incorrectly set to "1"
    in the running configuration
    and should have a value of: "0"
 - "net.ipv4.conf.all.send_redirects" is not set in an included file
    ** Note: "net.ipv4.conf.all.send_redirects" May be set in a file that's ignored by load
 procedure **
 - "net.ipv4.conf.default.send_redirects" is incorrectly set to "1"
    in the running configuration
    and should have a value of: "0"
 - "net.ipv4.conf.default.send_redirects" is not set in an included file
    ** Note: "net.ipv4.conf.default.send_redirects" May be set in a file that's ignored by load
 procedure **
```

## 3.3.5 Ensure icmp redirects are not accepted

### Info

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables.
ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables.
By setting net.ipv4.conf.all.accept_redirects net.ipv4.conf.default.accept_redirects net.ipv6.conf.all.accept_redirects and net.ipv6.conf.default.accept_redirects to 0 the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

### Solution

Set the following parameters in /etc/sysctl.conf or a file in /etc/sysctl.d/ ending inconf :
- net.ipv4.conf.all.accept_redirects = 0
- net.ipv4.conf.default.accept_redirects = 0

Example:
```
# printf '%s ' "net.ipv4.conf.all.accept_redirects = 0" "net.ipv4.conf.default.accept_redirects = 0" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```
Run the following script to set the active kernel parameters:
```
#!/usr/bin/env bash
{ sysctl -w net.ipv4.conf.all.accept_redirects=0 sysctl -w net.ipv4.conf.default.accept_redirects=0 sysctl -w net.ipv4.route.flush=1 }
```
- IF - IPv6 is enabled on the system:

Set the following parameters in /etc/sysctl.conf or a file in /etc/sysctl.d/ ending inconf :
- net.ipv6.conf.all.accept_redirects = 0
- net.ipv6.conf.default.accept_redirects = 0

Example:
```
# printf '%s ' "net.ipv6.conf.all.accept_redirects = 0" "net.ipv6.conf.default.accept_redirects = 0" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```
Run the following script to set the active kernel parameters:
```
#!/usr/bin/env bash
{ sysctl -w net.ipv6.conf.all.accept_redirects=0 sysctl -w net.ipv6.conf.default.accept_redirects=0 sysctl -w net.ipv6.route.flush=1 }
```
Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |

| | |
|---|---|
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:
 - "net.ipv4.conf.default.accept_redirects" is incorrectly set to "1"
    in the running configuration
    and should have a value of: "0"
 - "net.ipv6.conf.all.accept_redirects" is incorrectly set to "1"
    in the running configuration
    and should have a value of: "0"
 - "net.ipv6.conf.default.accept_redirects" is incorrectly set to "1"
    in the running configuration
    and should have a value of: "0"

- Correctly set:
 - "net.ipv4.conf.all.accept_redirects" is correctly set to "0"
    in the running configuration
 - "net.ipv4.conf.all.accept_redirects" is correctly set to "0"
    in "/etc/ufw/sysctl.conf"
 - "net.ipv4.conf.default.accept_redirects" is correctly set to "0"
    in "/etc/ufw/sysctl.conf"
 - "net.ipv6.conf.all.accept_redirects" is correctly set to "0"
    in "/etc/ufw/sysctl.conf"
 - "net.ipv6.conf.default.accept_redirects" is correctly set to "0"
    in "/etc/ufw/sysctl.conf"
```

## 3.3.6 Ensure secure icmp redirects are not accepted

### Info

Secure ICMP redirects are the same as ICMP redirects, except they come from gateways listed on the default gateway list. It is assumed that these gateways are known to your system, and that they are likely to be secure.
It is still possible for even known gateways to be compromised. Setting net.ipv4.conf.all.secure_redirects and net.ipv4.conf.default.secure_redirects to 0 protects the system from routing table updates by possibly compromised known gateways.

### Solution

Set the following parameters in /etc/sysctl.conf or a file in /etc/sysctl.d/ ending inconf :
- net.ipv4.conf.all.secure_redirects = 0
- net.ipv4.conf.default.secure_redirects = 0
Example:
# printf '%s ' "net.ipv4.conf.all.secure_redirects = 0" "net.ipv4.conf.default.secure_redirects = 0" >> /etc/sysctl.d/60-netipv4_sysctl.conf
Run the following script to set the active kernel parameters:
#!/usr/bin/env bash
{ sysctl -w net.ipv4.conf.all.secure_redirects=0 sysctl -w net.ipv4.conf.default.secure_redirects=0 sysctl -w net.ipv4.route.flush=1 }
Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |

| | |
|---|---|
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:
 - "net.ipv4.conf.all.secure_redirects" is incorrectly set to "1"
    in the running configuration
    and should have a value of: "0"
 - "net.ipv4.conf.all.secure_redirects" is not set in an included file
    ** Note: "net.ipv4.conf.all.secure_redirects" May be set in a file that's ignored by load
 procedure **
 - "net.ipv4.conf.default.secure_redirects" is incorrectly set to "1"
    in the running configuration
    and should have a value of: "0"
 - "net.ipv4.conf.default.secure_redirects" is not set in an included file
    ** Note: "net.ipv4.conf.default.secure_redirects" May be set in a file that's ignored by load
 procedure **
```

## 3.3.7 Ensure reverse path filtering is enabled

### Info

Setting net.ipv4.conf.all.rp_filter and net.ipv4.conf.default.rp_filter to 1 forces the Linux kernel to utilize reverse path filtering on a received packet to determine if the packet was valid. Essentially, with reverse path filtering, if the return packet does not go out the same interface that the corresponding source packet came from, the packet is dropped (and logged if log_martians is set).
Setting net.ipv4.conf.all.rp_filter and net.ipv4.conf.default.rp_filter to 1 is a good way to deter attackers from sending your system bogus packets that cannot be responded to. One instance where this feature breaks down is if asymmetrical routing is employed. This would occur when using dynamic routing protocols (bgp, ospf, etc) on your system. If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

### Solution

Set the following parameters in /etc/sysctl.conf or a file in /etc/sysctl.d/ ending inconf :
- net.ipv4.conf.all.rp_filter = 1
- net.ipv4.conf.default.rp_filter = 1
Example:
# printf '%s ' "net.ipv4.conf.all.rp_filter = 1" "net.ipv4.conf.default.rp_filter = 1" >> /etc/sysctl.d/60-netipv4_sysctl.conf
Run the following script to set the active kernel parameters:
#!/usr/bin/env bash
{ sysctl -w net.ipv4.conf.all.rp_filter=1 sysctl -w net.ipv4.conf.default.rp_filter=1 sysctl -w net.ipv4.route.flush=1 }
Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten
Impact:
If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |

| | |
|---|---|
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:
 - "net.ipv4.conf.all.rp_filter" is incorrectly set to "2"
    in the running configuration
    and should have a value of: "1"
 - "net.ipv4.conf.all.rp_filter" is incorrectly set to "2"
    in "/etc/sysctl.d/10-network-security.conf"
    and should have a value of: "1"
 - "net.ipv4.conf.default.rp_filter" is incorrectly set to "2"
    in the running configuration
    and should have a value of: "1"
 - "net.ipv4.conf.default.rp_filter" is incorrectly set to "2"
    in "/etc/sysctl.d/10-network-security.conf"
    and should have a value of: "1"
```

## 3.3.8 Ensure source routed packets are not accepted

### Info

In networking, source routing allows a sender to partially or fully specify the route packets take through a network. In contrast, non-source routed packets travel a path determined by routers in the network. In some cases, systems may not be routable or reachable from some locations (e.g. private addresses vs. Internet routable), and so source routed packets would need to be used.
Setting net.ipv4.conf.all.accept_source_route net.ipv4.conf.default.accept_source_route net.ipv6.conf.all.accept_source_route and net.ipv6.conf.default.accept_source_route to 0 disables the system from accepting source routed packets. Assume this system was capable of routing packets to Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

### Solution

Set the following parameters in /etc/sysctl.conf or a file in /etc/sysctl.d/ ending inconf :
- net.ipv4.conf.all.accept_source_route = 0
- net.ipv4.conf.default.accept_source_route = 0
Example:
# printf '%s ' "net.ipv4.conf.all.accept_source_route = 0" "net.ipv4.conf.default.accept_source_route = 0" >> /etc/sysctl.d/60-netipv4_sysctl.conf
Run the following script to set the active kernel parameters:
#!/usr/bin/env bash
{ sysctl -w net.ipv4.conf.all.accept_source_route=0 sysctl -w net.ipv4.conf.default.accept_source_route=0 sysctl -w net.ipv4.route.flush=1 }
- IF - IPv6 is enabled on the system:
Set the following parameters in /etc/sysctl.conf or a file in /etc/sysctl.d/ ending inconf :
- net.ipv6.conf.all.accept_source_route = 0
- net.ipv6.conf.default.accept_source_route = 0
Example:
# printf '%s ' "net.ipv6.conf.all.accept_source_route = 0" "net.ipv6.conf.default.accept_source_route = 0" >> /etc/sysctl.d/60-netipv6_sysctl.conf
Run the following command to set the active kernel parameters:
#!/usr/bin/env bash
{ sysctl -w net.ipv6.conf.all.accept_source_route=0 sysctl -w net.ipv6.conf.default.accept_source_route=0 sysctl -w net.ipv6.route.flush=1 }
Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |

| | |
|---|---|
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:
 - "net.ipv4.conf.all.accept_source_route" is not set in an included file
    ** Note: "net.ipv4.conf.all.accept_source_route" May be set in a file that's ignored by load
 procedure **
 - "net.ipv4.conf.default.accept_source_route" is incorrectly set to "1"
    in the running configuration
    and should have a value of: "0"
 - "net.ipv4.conf.default.accept_source_route" is not set in an included file
    ** Note: "net.ipv4.conf.default.accept_source_route" May be set in a file that's ignored by
 load procedure **
 - "net.ipv6.conf.all.accept_source_route" is not set in an included file
    ** Note: "net.ipv6.conf.all.accept_source_route" May be set in a file that's ignored by load
 procedure **
 - "net.ipv6.conf.default.accept_source_route" is not set in an included file
    ** Note: "net.ipv6.conf.default.accept_source_route" May be set in a file that's ignored by
 load procedure **

- Correctly set:
 - "net.ipv4.conf.all.accept_source_route" is correctly set to "0"
    in the running configuration
 - "net.ipv6.conf.all.accept_source_route" is correctly set to "0"
    in the running configuration
 - "net.ipv6.conf.default.accept_source_route" is correctly set to "0"
    in the running configuration
```

## 3.3.9 Ensure suspicious packets are logged

### Info

When enabled, this feature logs packets with un-routable source addresses to the kernel log.
Setting net.ipv4.conf.all.log_martians and net.ipv4.conf.default.log_martians to 1 enables this feature. Logging these packets allows an administrator to investigate the possibility that an attacker is sending spoofed packets to their system.

### Solution

Set the following parameters in /etc/sysctl.conf or a file in /etc/sysctl.d/ ending inconf :
- net.ipv4.conf.all.log_martians = 1
- net.ipv4.conf.default.log_martians = 1

Example:

```
# printf '%s ' "net.ipv4.conf.all.log_martians = 1" "net.ipv4.conf.default.log_martians = 1" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

```
#!/usr/bin/env bash
{ sysctl -w net.ipv4.conf.all.log_martians=1 sysctl -w net.ipv4.conf.default.log_martians=1 sysctl -w net.ipv4.route.flush=1 }
```

Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171** | 3.3.6 |
| **800-171R3** | 03.03.02a. |
| **800-171R3** | 03.03.02b. |
| **800-171R3** | 03.03.03 |
| **800-171R3** | 03.03.06a. |
| **800-53** | AU-3 |
| **800-53** | AU-3(1) |
| **800-53** | AU-7 |
| **800-53** | AU-12 |
| **800-53R5** | AU-3 |
| **800-53R5** | AU-3(1) |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-12 |
| **CN-L3** | 7.1.2.3(a) |
| **CN-L3** | 7.1.2.3(b) |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 7.1.3.3(a) |

| | |
|---|---|
| **CN-L3** | 7.1.3.3(b) |
| **CN-L3** | 8.1.4.3(b) |
| **CSCV7** | 6.2 |
| **CSCV7** | 6.3 |
| **CSCV8** | 8.5 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | DE.CM-7 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.5.28 |
| **ISO-27001-2022** | A.8.15 |
| **ITSG-33** | AU-3 |
| **ITSG-33** | AU-3(1) |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-12 |
| **LEVEL** | 1A |
| **NESA** | T3.6.2 |
| **NIAV2** | AM34a |
| **NIAV2** | AM34b |
| **NIAV2** | AM34c |

| | |
|---|---|
| **NIAV2** | AM34d |
| **NIAV2** | AM34e |
| **NIAV2** | AM34f |
| **NIAV2** | AM34g |
| **PCI-DSSV3.2.1** | 10.1 |
| **PCI-DSSV3.2.1** | 10.3 |
| **PCI-DSSV3.2.1** | 10.3.1 |
| **PCI-DSSV3.2.1** | 10.3.2 |
| **PCI-DSSV3.2.1** | 10.3.3 |
| **PCI-DSSV3.2.1** | 10.3.4 |
| **PCI-DSSV3.2.1** | 10.3.5 |
| **PCI-DSSV3.2.1** | 10.3.6 |
| **PCI-DSSV4.0** | 10.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:
 - "net.ipv4.conf.all.log_martians" is incorrectly set to "0"
    in the running configuration
    and should have a value of: "1"
 - "net.ipv4.conf.all.log_martians" is incorrectly set to "0"
    in "/etc/ufw/sysctl.conf"
    and should have a value of: "1"
 - "net.ipv4.conf.default.log_martians" is incorrectly set to "0"
    in the running configuration
    and should have a value of: "1"
 - "net.ipv4.conf.default.log_martians" is incorrectly set to "0"
    in "/etc/ufw/sysctl.conf"
    and should have a value of: "1"
```

## 4.4.2.1 Ensure iptables default deny firewall policy

### Info

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.
Notes:
- Changing firewall settings while connected over network can result in being locked out of the system
- Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well
With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to allow list acceptable usage than to deny list unacceptable usage.

### Solution

Run the following commands to implement a default DROP policy:
# iptables -P INPUT DROP # iptables -P OUTPUT DROP # iptables -P FORWARD DROP

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |
| **CSF2.0** | DE.CM-01 |

| | |
|---|---|
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |

| | |
|---|---|
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - iptables Chain FORWARD
The command '/sbin/iptables -L -n | /bin/grep 'Chain FORWARD'' returned :

# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain FORWARD (policy DROP)

-------------------------
FAILED - iptables Chain INPUT
The command '/sbin/iptables -L -n | /bin/grep 'Chain INPUT'' returned :

# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain INPUT (policy ACCEPT)

-------------------------
FAILED - iptables Chain OUTPUT
The command '/sbin/iptables -L -n | /bin/grep 'Chain OUTPUT'' returned :

# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain OUTPUT (policy ACCEPT)
```

## 4.4.2.2 Ensure iptables loopback traffic is configured

### Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8).
Note:
- Changing firewall settings while connected over network can result in being locked out of the system
- Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well
Loopback traffic is generated between processes on machine and is typically critical to the operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

### Solution

Run the following commands to implement the loopback rules:
# iptables -A INPUT -i lo -j ACCEPT # iptables -A OUTPUT -o lo -j ACCEPT # iptables -A INPUT -s 127.0.0.0/8 -j DROP

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |

| | |
|---|---|
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |

| | |
|---|---|
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - iptables INPUT
The command '/sbin/iptables -L INPUT -v -n | /bin/awk '{ a[$3":"$4":"$6":"$7":"$8":"$9]
 = NR; print } END { if (a["ACCEPT:0:lo:*:0.0.0.0/0:0.0.0.0/0"] > 0 &&
 a["ACCEPT:0:lo:*:0.0.0.0/0:0.0.0.0/0"] < a["DROP:0:*:*:127.0.0.0/8:0.0.0.0/0"]) { print "pass" }
 else { print "fail" } }'' returned :

# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain INPUT (policy ACCEPT 14M packets, 2011M bytes)
 pkts bytes target     prot opt in     out     source               destination
fail

-------------------------
FAILED - iptables OUTPUT
The command '/sbin/iptables -L OUTPUT -v -n | /bin/awk '{ a[$3":"$4":"$6":"$7":"$8":"$9] = NR;
 print } END { if (a["ACCEPT:0:*:lo:0.0.0.0/0:0.0.0.0/0"] > 0) { print "pass" } else { print
 "fail" } }'' returned :

# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain OUTPUT (policy ACCEPT 5034K packets, 2881M bytes)
 pkts bytes target     prot opt in     out     source               destination
fail
```

## 4.4.3.1 Ensure ip6tables default deny firewall policy

### Info

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.
Note:
- Changing firewall settings while connected over network can result in being locked out of the system
- Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well
With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to allow list acceptable usage than to deny list unacceptable usage.

### Solution

- IF - IPv6 is enabled on your system:
Run the following commands to implement a default DROP policy:
# ip6tables -P INPUT DROP # ip6tables -P OUTPUT DROP # ip6tables -P FORWARD DROP

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |

| | |
|---|---|
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |

| | |
|---|---|
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - ip6tables Chain INPUT DROP REJECT
The command '/sbin/ip6tables -L -n | /bin/grep 'Chain INPUT'' returned :

Chain INPUT (policy ACCEPT)

-------------------------
FAILED - ip6tables Chain OUTPUT DROP REJECT
The command '/sbin/ip6tables -L -n | /bin/grep 'Chain OUTPUT'' returned :

Chain OUTPUT (policy ACCEPT)

-------------------------
FAILED - ip6tables Chain FORWARD DROP REJECT
The command '/sbin/ip6tables -L -n | /bin/grep 'Chain FORWARD'' returned :

Chain FORWARD (policy ACCEPT)
```

## 4.4.3.2 Ensure ip6tables loopback traffic is configured

### Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (::1).
Note:
- Changing firewall settings while connected over network can result in being locked out of the system
- Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well
Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (::1) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

### Solution

Run the following commands to implement the loopback rules:
# ip6tables -A INPUT -i lo -j ACCEPT # ip6tables -A OUTPUT -o lo -j ACCEPT # ip6tables -A INPUT -s ::1 -j DROP

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |

| | |
|---|---|
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |

|  |  |
|---|---|
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - ip6tables input
The command '/sbin/ip6tables -L INPUT -v -n | /bin/awk '{ a[$3":"$4":"$6":"$7":"$8":"$9] =
 NR; print } END { if (a["ACCEPT:0:lo:*:::/0:::/0"] > 0 && a["ACCEPT:0:lo:*:::/0:::/0"] <
 a["DROP:0:*:*:::1:::/0"]) { print "pass" } else { print "fail" } }'' returned :

Chain INPUT (policy ACCEPT 12M packets, 1575M bytes)
 pkts bytes target     prot opt in     out     source               destination
fail

-------------------------
FAILED - ip6tables output
The command '/sbin/ip6tables -L OUTPUT -v -n | /bin/awk '{ a[$3":"$4":"$6":"$7":"$8":"$9] = NR;
 print } END { if (a["ACCEPT:0:*:lo:::/0:::/0"] > 0) { print "pass" } else { print "fail" } }''
 returned :

Chain OUTPUT (policy ACCEPT 198K packets, 1945M bytes)
 pkts bytes target     prot opt in     out     source               destination
fail
```

## 4.4.3.4 Ensure ip6tables firewall rules exist for all open ports

### Info

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.
Notes:
- Changing firewall settings while connected over network can result in being locked out of the system
- Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well
- The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy
Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

### Solution

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:

```
# ip6tables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j ACCEPT
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |

| | |
|---|---|
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |

| | |
|---|---|
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

### Assets

#### linux_project

```
The command script with multiple lines returned :

FAILED: The following open port(s) dont have a firewall rule: "443", "7946", "11434", "80", "22",
 "443", "2377", "3000", "7946"
```

## 5.1.1 Ensure permissions on /etc/ssh/sshd_config are configured

### Info

The file /etc/ssh/sshd_config and files ending inconf in the /etc/ssh/sshd_config.d directory, contain configuration specifications for sshd
configuration specifications for sshd need to be protected from unauthorized changes by non-privileged users.

### Solution

Run the following script to set ownership and permissions on /etc/ssh/sshd_config and files ending inconf in the /etc/ssh/sshd_config.d directory:

```
#!/usr/bin/env bash
{ chmod u-x,og-rwx /etc/ssh/sshd_config chown root:root /etc/ssh/sshd_config while IFS= read -r -d $'0' l_file; do if [ -e "$l_file" ]; then chmod u-x,og-rwx "$l_file"
chown root:root "$l_file"
fi done < <(find /etc/ssh/sshd_config.d -type f -print0 2>/dev/null) }
```

- IF - other locations are listed in an Include statement, *.conf files in these locations access should also be modified.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |

| | |
|---|---|
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |

| | |
|---|---|
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |

| | |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - * Reasons for audit failure * :

 - File: "/etc/ssh/sshd_config":
  - Is mode: "0644" should be: "600" or more restrictive
 - File: "/etc/ssh/sshd_config.d/60-cloudimg-settings.conf":
  - Is mode: "0644" should be: "600" or more restrictive
```

## 5.1.13 Ensure sshd LoginGraceTime is configured

### Info

The LoginGraceTime parameter specifies the time allowed for successful authentication to the SSH server. The longer the Grace period is the more open unauthenticated connections can exist. Like other session controls in this session the Grace Period should be limited to appropriate organizational limits to ensure the service is available for needed access.
Setting the LoginGraceTime parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. It will also limit the number of concurrent unauthenticated connections While the recommended setting is 60 seconds (1 Minute), set the number based on site policy.

### Solution

Edit the /etc/ssh/sshd_config file to set the LoginGraceTime parameter to 60 seconds or less above any Include entry as follows:
LoginGraceTime 60
Note: First occurrence of a option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.11 |
| **800-171R3** | 03.01.11 |
| **800-53** | AC-10 |
| **800-53** | AC-12 |
| **800-53R5** | AC-10 |
| **800-53R5** | AC-12 |
| **CN-L3** | 7.1.2.2(d) |
| **CN-L3** | 7.1.3.7(b) |
| **CN-L3** | 8.1.4.1(b) |
| **CSF2.0** | PR.AA-03 |
| **CSF2.0** | PR.AA-05 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(iii) |
| **ITSG-33** | AC-10 |
| **ITSG-33** | AC-12 |
| **LEVEL** | 1A |
| **NESA** | T5.5.1 |
| **NIAV2** | NS49 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |

## Assets

### linux_project

```
The command script with multiple lines returned :

port 22: logingracetime 120
Fail
```

## 5.1.15 Ensure sshd MACs are configured

### Info

This variable limits the types of MAC algorithms that SSH can use during communication.
Notes:
- Some organizations may have stricter requirements for approved MACs.
- Ensure that MACs used are in compliance with site policy.
- The only "strong" MACs currently FIPS 140 approved are:
- HMAC-SHA1
- HMAC-SHA2-256
- HMAC-SHA2-384
- HMAC-SHA2-512
MD5 and 96-bit MAC algorithms are considered weak and have been shown to increase exploitability in SSH downgrade attacks. Weak algorithms continue to have a great deal of attention as a weak spot that can be exploited with expanded computing power. An attacker that breaks the algorithm could take advantage of a MiTM position to decrypt the SSH tunnel and capture credentials and information.

### Solution

Edit the /etc/ssh/sshd_config file and add/modify the MACs line to contain a comma separated list of the site unapproved (weak) MACs preceded with a - above any Include entries:
Example:
MACs -hmac-md5,hmac-md5-96,hmac-ripemd160,hmac-sha1-96,umac-64@openssh.com,hmac-md5-etm@openssh.com,hmac-md5-96-etm@openssh.com,hmac-ripemd160-etm@openssh.com,hmac-sha1-96-etm@openssh.com,umac-64-etm@openssh.com,umac-128-etm@openssh.com
- IF - CVE-2023-48795 has not been reviewed and addressed, the following etm MACs should be added to the exclude list:
hmac-sha1-etm@openssh.com
,
hmac-sha2-256-etm@openssh.com
,
hmac-sha2-512-etm@openssh.com
Note: First occurrence of an option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.13 |
| **800-171** | 3.5.2 |
| **800-171** | 3.13.8 |
| **800-171R3** | 03.05.07 |
| **800-171R3** | 03.05.12 |
| **800-171R3** | 03.13.08 |
| **800-53** | AC-17(2) |
| **800-53** | IA-5 |
| **800-53** | IA-5(1) |
| **800-53** | SC-8 |
| **800-53** | SC-8(1) |
| **800-53R5** | AC-17(2) |
| **800-53R5** | IA-5 |

| | |
|---|---|
| **800-53R5** | IA-5(1) |
| **800-53R5** | SC-8 |
| **800-53R5** | SC-8(1) |
| **CN-L3** | 7.1.2.7(g) |
| **CN-L3** | 7.1.3.1(d) |
| **CN-L3** | 8.1.2.2(a) |
| **CN-L3** | 8.1.2.2(b) |
| **CN-L3** | 8.1.4.1(c) |
| **CN-L3** | 8.1.4.7(a) |
| **CN-L3** | 8.1.4.8(a) |
| **CN-L3** | 8.2.4.5(c) |
| **CN-L3** | 8.2.4.5(d) |
| **CN-L3** | 8.5.2.2 |
| **CSCV7** | 14.4 |
| **CSCV7** | 16.5 |
| **CSCV8** | 3.10 |
| **CSF** | PR.AC-1 |
| **CSF** | PR.AC-3 |
| **CSF** | PR.DS-2 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-02 |
| **GDPR** | 32.1.a |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |

| | |
|---|---|
| **HIPAA** | 164.312(e)(1) |
| **HIPAA** | 164.312(e)(2)(i) |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.6.7 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.2.2 |
| **ISO/IEC-27001** | A.10.1.1 |
| **ISO/IEC-27001** | A.13.2.3 |
| **ITSG-33** | AC-17(2) |
| **ITSG-33** | IA-5 |
| **ITSG-33** | IA-5(1) |
| **ITSG-33** | SC-8 |
| **ITSG-33** | SC-8a. |
| **ITSG-33** | SC-8(1) |
| **LEVEL** | 1A |
| **NESA** | T4.3.1 |
| **NESA** | T4.3.2 |
| **NESA** | T4.5.1 |
| **NESA** | T4.5.2 |
| **NESA** | T5.2.3 |
| **NESA** | T5.4.2 |
| **NESA** | T7.3.3 |
| **NESA** | T7.4.1 |
| **NIAV2** | AM37 |
| **NIAV2** | IE8 |
| **NIAV2** | IE9 |
| **NIAV2** | IE12 |

| | |
|---|---|
| **NIAV2** | NS5d |
| **NIAV2** | NS6b |
| **NIAV2** | NS29 |
| **NIAV2** | SS24 |
| **PCI-DSSV3.2.1** | 2.3 |
| **PCI-DSSV3.2.1** | 4.1 |
| **PCI-DSSV4.0** | 2.2.7 |
| **PCI-DSSV4.0** | 4.2.1 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 2.1 |
| **SWIFT-CSCV1** | 2.6 |
| **SWIFT-CSCV1** | 4.1 |
| **TBA-FIISB** | 29.1 |

## Assets

### linux_project

```
The command script with multiple lines returned :

port 22: macs umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-
sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-
sha2-256,hmac-sha2-512,hmac-sha1
Fail
```

## 5.1.16 Ensure sshd MaxAuthTries is configured

### Info

The MaxAuthTries parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the syslog file detailing the login failure.
Setting the MaxAuthTries parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, set the number based on site policy.

### Solution

Edit the /etc/ssh/sshd_config file to set the MaxAuthTries parameter to 4 or less above any Include and Match entries as follows:
MaxAuthTries 4
Note: First occurrence of an option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171** | 3.3.6 |
| **800-171R3** | 03.03.02a. |
| **800-171R3** | 03.03.02b. |
| **800-171R3** | 03.03.03 |
| **800-171R3** | 03.03.06a. |
| **800-53** | AU-3 |
| **800-53** | AU-3(1) |
| **800-53** | AU-7 |
| **800-53** | AU-12 |
| **800-53R5** | AU-3 |
| **800-53R5** | AU-3(1) |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-12 |
| **CN-L3** | 7.1.2.3(a) |
| **CN-L3** | 7.1.2.3(b) |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 7.1.3.3(a) |
| **CN-L3** | 7.1.3.3(b) |
| **CN-L3** | 8.1.4.3(b) |

| | |
|---|---|
| **CSCV7** | 16.13 |
| **CSCV8** | 8.5 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | DE.CM-7 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.5.28 |
| **ISO-27001-2022** | A.8.15 |
| **ITSG-33** | AU-3 |
| **ITSG-33** | AU-3(1) |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-12 |
| **LEVEL** | 1A |
| **NESA** | T3.6.2 |
| **NIAV2** | AM34a |
| **NIAV2** | AM34b |
| **NIAV2** | AM34c |
| **NIAV2** | AM34d |
| **NIAV2** | AM34e |
| **NIAV2** | AM34f |

| | |
|---|---|
| **NIAV2** | AM34g |
| **PCI-DSSV3.2.1** | 10.1 |
| **PCI-DSSV3.2.1** | 10.3 |
| **PCI-DSSV3.2.1** | 10.3.1 |
| **PCI-DSSV3.2.1** | 10.3.2 |
| **PCI-DSSV3.2.1** | 10.3.3 |
| **PCI-DSSV3.2.1** | 10.3.4 |
| **PCI-DSSV3.2.1** | 10.3.5 |
| **PCI-DSSV3.2.1** | 10.3.6 |
| **PCI-DSSV4.0** | 10.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |

## Assets

### linux_project

```
The command script with multiple lines returned :

port 22: maxauthtries 6
Fail
```

## 5.1.18 Ensure sshd MaxStartups is configured

### Info

The MaxStartups parameter specifies the maximum number of concurrent unauthenticated connections to the SSH daemon.
To protect a system from denial of service due to a large number of pending authentication connection attempts, use the rate limiting function of MaxStartups to protect availability of sshd logins and prevent overwhelming the daemon.

### Solution

Edit the /etc/ssh/sshd_config file to set the MaxStartups parameter to 10:30:60 or more restrictive above any Include entries as follows:
MaxStartups 10:30:60
Note: First occurrence of a option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-53** | AC-10 |
| **800-53R5** | AC-10 |
| **CSF2.0** | PR.AA-05 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ITSG-33** | AC-10 |
| **LEVEL** | 1A |
| **NESA** | T5.5.1 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |

### Assets

#### linux_project

```
The command script with multiple lines returned :

port 22: maxstartups 10:30:100
Fail
```

## 5.1.20 Ensure sshd PermitRootLogin is disabled

### Info

The PermitRootLogin parameter specifies if the root user can log in using SSH. The default is prohibit-password Disallowing root logins over SSH requires system admins to authenticate using their own individual account, then escalating to root This limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident.

### Solution

Edit the /etc/ssh/sshd_config file to set the PermitRootLogin parameter to no above any Include and Match entries as follows:
PermitRootLogin no
Note: First occurrence of an option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.5 |
| **800-171** | 3.1.6 |
| **800-171R3** | 03.01.06a. |
| **800-171R3** | 03.01.06b. |
| **800-53** | AC-6(2) |
| **800-53** | AC-6(5) |
| **800-53R5** | AC-6(2) |
| **800-53R5** | AC-6(5) |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.10.6(a) |
| **CSCV7** | 4.3 |
| **CSCV8** | 5.4 |
| **CSF** | PR.AC-4 |
| **CSF2.0** | PR.AA-05 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.8.2 |

| | |
|---|---|
| **ISO-27001-2022** | A.8.18 |
| **ISO/IEC-27001** | A.9.2.3 |
| **ITSG-33** | AC-6(2) |
| **ITSG-33** | AC-6(5) |
| **LEVEL** | 1A |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.6.1 |
| **NIAV2** | AM1 |
| **NIAV2** | AM23f |
| **NIAV2** | AM32 |
| **NIAV2** | AM33 |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | VL3a |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **SWIFT-CSCV1** | 1.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

port 22: permitrootlogin yes
Fail
```

## 5.1.4 Ensure sshd access is configured

### Info

There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged:
- AllowUsers :
- The AllowUsers variable gives the system administrator the option of allowing specific users to ssh into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of user@host.
- AllowGroups :
- The AllowGroups variable gives the system administrator the option of allowing specific groups of users to ssh into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.
- DenyUsers :
- The DenyUsers variable gives the system administrator the option of denying specific users to ssh into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of user@host.
- DenyGroups :
- The DenyGroups variable gives the system administrator the option of denying specific groups of users to ssh into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.

Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

### Solution

Edit the /etc/ssh/sshd_config file to set one or more of the parameters above any Include and Match set statements as follows:
AllowUsers <userlist>
- AND/OR - AllowGroups <grouplist>
Note:
- First occurrence of a option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in aconf file in a Include directory.
- Be advised that these options are "ANDed" together. If both AllowUsers and AllowGroups are set, connections will be limited to the list of users that are also a member of an allowed group. It is recommended that only one be set for clarity and ease of administration.
- It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user or group and forget to add it to the deny list.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |

| | |
|---|---|
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 4.3 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |

| | |
|---|---|
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |

| | |
|---|---|
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

port 22:
Fail
```

## 5.1.5 Ensure sshd Banner is configured

### Info

The Banner parameter specifies a file whose contents must be sent to the remote user before authentication is permitted. By default, no banner is displayed.
Banners are used to warn connecting users of the particular site's policy regarding connection. Presenting a warning message prior to the normal user login may assist the prosecution of trespassers on the computer system.

### Solution

Edit the /etc/ssh/sshd_config file to set the Banner parameter above any Include and Match entries as follows:
Banner /etc/issue.net
Note: First occurrence of a option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.
Edit the file being called by the Banner argument with the appropriate contents according to your site policy, remove any instances of m r s v or references to the OS platform
Example:
# printf '%s ' "Authorized users only. All activity may be monitored and reported." > "$(sshd -T | awk '$1 == "banner" {print $2}')"

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.9 |
| **800-171R3** | 03.01.09 |
| **800-53** | AC-8 |
| **800-53R5** | AC-8 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.5 |
| **ITSG-33** | AC-8 |
| **LEVEL** | 1A |
| **NESA** | M1.3.6 |
| **TBA-FIISB** | 45.2.4 |

### Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - Ensure banner is set to /etc/issue.net
The command script with multiple lines returned :

port 22: banner none
Fail

-------------------------
PASSED - Ensure any instances of m, s, r, v or any references to the OS platform are removed
 from /etc/issue.net
The command '/bin/grep -Psi -- "(\\\v|\\\r|\\\m|\\\s|\b$(/bin/grep '^ID=' /etc/os-release | /bin/
cut -d= -f2 | /bin/sed -e 's/"//g')\b)" "$(/sbin/sshd -T | /bin/awk '$1 == "banner" {print $2}')"
 | /bin/awk '{ print } END { if(NR==0) print "Pass"; else print "Fail" }'' returned :

Pass
```

```
-------------------------
FAILED - Ensure banner argument matches site policy
First ERROR: Ubuntu 24.04.2 != All activities
Ubuntu 24.04.2 LTS
```

## 5.1.7 Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured

### Info

Note: To clarify, the two settings described below are only meant for idle connections from a protocol perspective and are not meant to check if the user is active or not. An idle user does not mean an idle connection. SSH does not and never had, intentionally, the capability to drop idle users. In SSH versions before 8.2p1 there was a bug that caused these values to behave in such a manner that they were abused to disconnect idle users. This bug has been resolved in 8.2p1 and thus it can no longer be abused disconnect idle users.
The two options ClientAliveInterval and ClientAliveCountMax control the timeout of SSH sessions. Taken directly from man 5 sshd_config :
-
ClientAliveInterval Sets a timeout interval in seconds after which if no data has been received from the client, sshd(8) will send a message through the encrypted channel to request a response from the client. The default is 0, indicating that these messages will not be sent to the client.
-
ClientAliveCountMax Sets the number of client alive messages which may be sent without sshd(8) receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, sshd will disconnect the client, terminating the session. It is important to note that the use of client alive messages is very different from TCPKeepAlive. The client alive messages are sent through the encrypted channel and therefore will not be spoofable. The TCP keepalive option en-abled by TCPKeepAlive is spoofable. The client alive mechanism is valuable when the client or server depend on knowing when a connection has become unresponsive.The default value is 3. If ClientAliveInterval is set to 15, and ClientAliveCountMax is left at the default, unresponsive SSH clients will be disconnected after approximately 45 seconds. Setting a zero ClientAliveCountMax disables connection termination.
In order to prevent resource exhaustion, appropriate values should be set for both ClientAliveInterval and ClientAliveCountMax Specifically, looking at the source code, ClientAliveCountMax must be greater than zero in order to utilize the ability of SSH to drop idle connections. If connections are allowed to stay open indefinitely, this can potentially be used as a DDOS attack or simple resource exhaustion could occur over unreliable networks.
The example set here is a 45 second timeout. Consult your site policy for network timeouts and apply as appropriate.

### Solution

Edit the /etc/ssh/sshd_config file to set the ClientAliveInterval and ClientAliveCountMax parameters above any Include and Match entries according to site policy.
Example:
ClientAliveInterval 15 ClientAliveCountMax 3
Note: First occurrence of a option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.11 |
| **800-171R3** | 03.01.11 |
| **800-53** | AC-12 |
| **800-53R5** | AC-12 |
| **CN-L3** | 7.1.2.2(d) |
| **CN-L3** | 7.1.3.7(b) |
| **CN-L3** | 8.1.4.1(b) |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(iii) |

| | |
|---|---|
| **ITSG-33** | AC-12 |
| **LEVEL** | 1A |
| **NIAV2** | NS49 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - ClientAliveCountMax is greater than 0
The command script with multiple lines returned :

port 22: clientalivecountmax 3
Pass

-------------------------
FAILED - ClientAliveInterval is greater than 0
The command script with multiple lines returned :

port 22: clientaliveinterval 0
Fail
```

## 5.2.3 Ensure sudo log file exists

### Info

sudo can use a custom log file
A sudo log file simplifies auditing of sudo commands

### Solution

Edit the file /etc/sudoers or a file in /etc/sudoers.d/ with visudo or visudo -f <PATH TO FILE> and add the following line:
Example:
Defaults logfile="/var/log/sudo.log"
Note:
- sudo will read each file in /etc/sudoers.d skipping file names that end in ~ or contain a character to avoid causing problems with package manager or editor temporary/backup files.
- Files are parsed in sorted lexical order. That is, /etc/sudoers.d/01_first will be parsed before /etc/sudoers.d/10_second
- Be aware that because the sorting is lexical, not numeric, /etc/sudoers.d/1_whoops would be loaded after /etc/sudoers.d/10_second
- Using a consistent number of leading zeroes in the file names can be used to avoid such problems.
Impact:
WARNING: Editing the sudo configuration incorrectly can cause sudo to stop functioning. Always use visudo to modify sudo configuration files.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171** | 3.3.6 |
| **800-171R3** | 03.03.02a. |
| **800-171R3** | 03.03.02b. |
| **800-171R3** | 03.03.03 |
| **800-171R3** | 03.03.06a. |
| **800-53** | AU-3 |
| **800-53** | AU-3(1) |
| **800-53** | AU-7 |
| **800-53** | AU-12 |
| **800-53R5** | AU-3 |
| **800-53R5** | AU-3(1) |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-12 |
| **CN-L3** | 7.1.2.3(a) |
| **CN-L3** | 7.1.2.3(b) |
| **CN-L3** | 7.1.2.3(c) |

| | |
|---|---|
| **CN-L3** | 7.1.3.3(a) |
| **CN-L3** | 7.1.3.3(b) |
| **CN-L3** | 8.1.4.3(b) |
| **CSCV7** | 6.3 |
| **CSCV8** | 8.5 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | DE.CM-7 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.5.28 |
| **ISO-27001-2022** | A.8.15 |
| **ITSG-33** | AU-3 |
| **ITSG-33** | AU-3(1) |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-12 |
| **LEVEL** | 1A |
| **NESA** | T3.6.2 |
| **NIAV2** | AM34a |
| **NIAV2** | AM34b |
| **NIAV2** | AM34c |

| | |
|---|---|
| **NIAV2** | AM34d |
| **NIAV2** | AM34e |
| **NIAV2** | AM34f |
| **NIAV2** | AM34g |
| **PCI-DSSV3.2.1** | 10.1 |
| **PCI-DSSV3.2.1** | 10.3 |
| **PCI-DSSV3.2.1** | 10.3.1 |
| **PCI-DSSV3.2.1** | 10.3.2 |
| **PCI-DSSV3.2.1** | 10.3.3 |
| **PCI-DSSV3.2.1** | 10.3.4 |
| **PCI-DSSV3.2.1** | 10.3.5 |
| **PCI-DSSV3.2.1** | 10.3.6 |
| **PCI-DSSV4.0** | 10.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |

### Assets

**linux_project**

```
No matching files were found
Less than 1 matches of regex found
```

## 5.2.7 Ensure access to the su command is restricted

### Info

The su command allows a user to run a command or shell as another user. The program has been superseded by sudo which allows for more granular control over privileged access. Normally, the su command can be executed by any user. By uncommenting the pam_wheel.so statement in /etc/pam.d/su the su command will only allow users in a specific groups to execute su This group should be empty to reinforce the use of sudo for privileged access.
Restricting the use of su and using sudo in its place, provides system administrators better control of the escalation of user privileges to execute privileged commands. The sudo utility also provides a better logging and audit mechanism, as it can log each command executed via sudo whereas su can only record that a user executed the su program.

### Solution

Create an empty group that will be specified for use of the su command. The group should be named according to site policy.
Example:
# groupadd sugroup
Add the following line to the /etc/pam.d/su file, specifying the empty group:
auth required pam_wheel.so use_uid group=sugroup

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |

| | |
|---|---|
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |

| | |
|---|---|
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |

|  |  |
|---|---|
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The command 'sugroup=$(/bin/grep -Pi '^\h*auth\h+(?:required|requisite)\h+pam_wheel\.so\h+(?:[^#
\n\r]+\h+)?((?!\2)(use_uid\b|group=\H+\b))\h+(?:[^#\n\r]+\h+)?((?!\1)(use_uid\b|group=\H+\b))(\h
+.*)?$' /etc/pam.d/su | /bin/awk 'BEGIN { FS = "="} ; { print $2 }'); if [ ! -z $sugroup ]; then /
bin/grep $sugroup /etc/group | /bin/awk 'BEGIN { FS = ":" }; { print $4 }' | /bin/awk '{print} END
 {if (NF == 0) print "pass - group empty"; else print "fail - group not empty"}'; else echo "fail
 - sugroup not found in /etc/pam.d/su"; fi' returned :

fail - sugroup not found in /etc/pam.d/su
```

## 5.3.1.3 Ensure libpam-pwquality is installed

### Info

libpwquality provides common functions for password quality checking and scoring them based on their apparent randomness. The library also provides a function for generating random passwords with good pronounceability.
This module can be plugged into the password stack of a given service to provide some plug-in strength-checking for passwords. The code was originally based on pam_cracklib module and the module is backwards compatible with its options.
Strong passwords reduce the risk of systems being hacked through brute force methods.

### Solution

Run the following command to install libpam-pwquality :
# apt install libpam-pwquality

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

### Assets

#### linux_project

```
The command '/bin/dpkg -s libpam-pwquality 2>&1 | /bin/grep -E '(Status:|not installed)''
 returned :

dpkg-query: package 'libpam-pwquality' is not installed and no information is available
```

## 5.3.2.2 Ensure pam_faillock module is enabled

### Info

The pam_faillock.so module maintains a list of failed authentication attempts per user during a specified interval and locks the account in case there were more than the configured number of consecutive failed authentications (this is defined by the deny parameter in the faillock configuration). It stores the failure records into per-user files in the tally directory.
Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

### Solution

Create two pam-auth-update profiles in /usr/share/pam-configs/ :
- Create the faillock profile in /usr/share/pam-configs/ with the following lines:
Name: Enable pam_faillock to deny access Default: yes Priority: 0 Auth-Type: Primary Auth:
[default=die] pam_faillock.so authfail
Example Script:
#!/usr/bin/env bash
{ arr=('Name: Enable pam_faillock to deny access' 'Default: yes' 'Priority: 0' 'Auth-Type: Primary' 'Auth:' ' [default=die] pam_faillock.so authfail') printf '%s ' "${arr[@]}" > /usr/share/pam-configs/faillock } <xhtml:ol start="2"> - Create the faillock_notify profile in /usr/share/pam-configs/ with the following lines:
Name: Notify of failed login attempts and reset count upon success Default: yes Priority: 1024 Auth-Type: Primary Auth:
requisite pam_faillock.so preauth Account-Type: Primary Account:
required pam_faillock.so
Example Script:
#!/usr/bin/env bash
{ arr=('Name: Notify of failed login attempts and reset count upon success' 'Default: yes' 'Priority: 1024' 'Auth-Type: Primary' 'Auth:' ' requisite pam_faillock.so preauth' 'Account-Type: Primary' 'Account:' ' required pam_faillock.so') printf '%s ' "${arr[@]}" > /usr/share/pam-configs/faillock_notify }
Run the following command to update the common-auth and common-account PAM files with the new profiles:
# pam-auth-update --enable <profile_filename>
Example:
# pam-auth-update --enable faillock # pam-auth-update --enable faillock_notify
Note:
- The name used for the file must be used in the pam-auth-update --enable command
- The Name: line should be easily recognizable and understood
- The Priority: Line is important as it effects the order of the lines in the /etc/pam.d/ files
- If a site specific custom profile is being used in your environment to configure PAM that includes the configuration for the pam_faillock module, enable that module instead

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171R3** | 03.01.01 |
| **800-171R3** | 03.15.01 |
| **800-53** | AC-1 |
| **800-53** | AC-2 |
| **800-53** | AC-2(1) |
| **800-53R5** | AC-1 |
| **800-53R5** | AC-2 |
| **800-53R5** | AC-2(1) |
| **CN-L3** | 7.1.3.2(d) |

| | |
|---|---|
| **CN-L3** | 8.1.4.2(e) |
| **CN-L3** | 8.1.10.6(c) |
| **CSCV7** | 16.7 |
| **CSCV8** | 6.2 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | ID.GV-1 |
| **CSF** | ID.GV-3 |
| **CSF** | PR.AC-1 |
| **CSF** | PR.AC-4 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | GV.OC-03 |
| **CSF2.0** | GV.OV-01 |
| **CSF2.0** | GV.PO-01 |
| **CSF2.0** | GV.PO-02 |
| **CSF2.0** | GV.SC-03 |
| **CSF2.0** | ID.IM-01 |
| **CSF2.0** | ID.IM-02 |
| **CSF2.0** | ID.IM-03 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.1 |
| **ISO-27001-2022** | A.5.2 |
| **ISO-27001-2022** | A.5.4 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.16 |

| | |
|---|---|
| **ISO-27001-2022** | A.5.18 |
| **ISO-27001-2022** | A.5.31 |
| **ISO-27001-2022** | A.5.36 |
| **ISO-27001-2022** | A.5.37 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | 5.2 |
| **ISO-27001-2022** | 5.3 |
| **ISO-27001-2022** | 7.5.1 |
| **ISO-27001-2022** | 7.5.2 |
| **ISO-27001-2022** | 7.5.3 |
| **ISO/IEC-27001** | A.9.1.1 |
| **ISO/IEC-27001** | A.9.2.1 |
| **ITSG-33** | AC-1 |
| **ITSG-33** | AC-2 |
| **ITSG-33** | AC-2(1) |
| **LEVEL** | 1A |
| **NESA** | M1.2.2 |
| **NIAV2** | AM28 |
| **NIAV2** | AM29 |
| **NIAV2** | AM30 |
| **NIAV2** | NS5j |
| **NIAV2** | SS14e |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 13.2 |
| **QCSC-V1** | 15.2 |

### Assets

#### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - /etc/pam.d/common-account
The following file(s) do not contain "(?i)^\h*account\h+([^#\n\r]+)\h+pam_faillock\.so\b":
      /etc/pam.d/common-account

-------------------------
```

```
FAILED - /etc/pam.d/common-auth authfail
The following file(s) do not contain "(?i)^\h*auth\h+([^#\n\r]+)\h+pam_faillock\.so\h+([^#\n\r]+\h
+)?authfail\b":
      /etc/pam.d/common-auth

-------------------------
FAILED - /etc/pam.d/common-auth preauth
The following file(s) do not contain "(?i)^\h*auth\h+([^#\n\r]+)\h+pam_faillock\.so\h+([^#\n\r]+\h
+)?preauth\b":
      /etc/pam.d/common-auth
```

## 5.3.2.3 Ensure pam_pwquality module is enabled

### Info

The pam_pwquality.so module performs password quality checking. This module can be plugged into the password stack of a given service to provide strength-checking for passwords. The code was originally based on pam_cracklib module and the module is backwards compatible with its options.
The action of this module is to prompt the user for a password and check its strength against a system dictionary and a set of rules for identifying poor choices.
The first action is to prompt for a single password, check its strength and then, if it is considered strong, prompt for the password a second time (to verify that it was typed correctly on the first occasion). All being well, the password is passed on to subsequent modules to be installed as the new authentication token.
Use of a unique, complex passwords helps to increase the time and resources required to compromise the password.

### Solution

Run the following script to verify the pam_pwquality.so line exists in a pam-auth-update profile:
# grep -P -- 'bpam_pwquality.sob' /usr/share/pam-configs/*
Output should be similar to:
/usr/share/pam-configs/pwquality: requisite pam_pwquality.so retry=3 /usr/share/pam-configs/pwquality: requisite pam_pwquality.so retry=3
- IF - similar output is returned:
Run the following command to update /etc/pam.d/common-password with the returned profile:
# pam-auth-update --enable {PROFILE_NAME}
Example:
# pam-auth-update pwquality
- IF - similar output is NOT returned:
Create a pam-auth-update profile in /usr/share/pam-configs/ with the following lines:
Name: Pwquality password strength checking Default: yes Priority: 1024 Conflicts: cracklib Password-Type: Primary Password:
requisite pam_pwquality.so retry=3
Example:
#!/usr/bin/env bash
{ arr=('Name: Pwquality password strength checking' 'Default: yes' 'Priority: 1024' 'Conflicts: cracklib' 'Password-Type: Primary' 'Password:' ' requisite pam_pwquality.so retry=3') printf '%s ' "${arr[@]}" > /usr/share/pam-configs/pwquality }
Run the following command to update /etc/pam.d/common-password with the pwquality profile:
# pam-auth-update --enable pwquality
Note:
- The name used for the file must be used in the pam-auth-update --enable command
- The Name: line should be easily recognizable and understood
- The Priority: Line is important as it effects the order of the lines in the /etc/pam.d/ files
- If a site specific custom profile is being used in your environment to configure PAM that includes the configuration for the pam_pwquality module, enable that module instead

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |

|  |  |
|---|---|
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

## Assets

### linux_project

```
The following file(s) do not contain "(?i)^\h*password\h+(requisite|required)\h+pam_pwquality\.so
\b":
      /etc/pam.d/common-password
```

## 5.3.2.4 Ensure pam_pwhistory module is enabled

### Info

The pam_pwhistory.so module saves the last passwords for each user in order to force password change history and keep the user from alternating between the same password too frequently.
This module does not work together with kerberos. In general, it does not make much sense to use this module in conjunction with NIS or LDAP since the old passwords are stored on the local machine and are not available on another machine for password history checking.
Use of a unique, complex passwords helps to increase the time and resources required to compromise the password.

### Solution

Run the following script to verify the pam_pwquality.so line exists in a pam-auth-update profile:

```
# grep -P -- 'bpam_pwhistory.sob' /usr/share/pam-configs/*
```

Output should be similar to:

```
/usr/share/pam-configs/pwhistory: requisite pam_pwhistory.so remember=24 enforce_for_root try_first_pass use_authtok
```

- IF - similar output is returned:
Run the following command to update /etc/pam.d/common-password with the returned profile:

```
# pam-auth-update --enable {PROFILE_NAME}
```

Example:

```
# pam-auth-update pwhistory
```

- IF - similar output is NOT returned:
Create a pwhistory profile in /usr/share/pam-configs/ with the following lines:
Name: pwhistory password history checking Default: yes Priority: 1024 Password-Type: Primary Password: requisite pam_pwhistory.so remember=24 enforce_for_root try_first_pass use_authtok
Example Script:

```
#!/usr/bin/env bash
{ arr=('Name: pwhistory password history checking' 'Default: yes' 'Priority: 1024' 'Password-Type: Primary' 'Password:' ' requisite pam_pwhistory.so remember=24 enforce_for_root try_first_pass use_authtok') printf '%s ' "${arr[@]}" > /usr/share/pam-configs/pwhistory }
```

Run the following command to update /etc/pam.d/common-password with the pwhistory profile:

```
# pam-auth-update --enable pwhistory
```

Note:
- The name used for the file must be used in the pam-auth-update --enable command
- The Name: line should be easily recognizable and understood
- The Priority: Line is important as it effects the order of the lines in the /etc/pam.d/ files
- If a site specific custom profile is being used in your environment to configure PAM that includes the configuration for the pam_pwhistory module, enable that module instead

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |

|  |  |
|---|---|
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

## Assets

### linux_project

```
The following file(s) do not contain "(?i)^\h*password\h+(requisite|required)\h+pam_pwhistory\.so
\b":
      /etc/pam.d/common-password
```

## 5.3.3.1.1 Ensure password failed attempts lockout is configured

### Info

The deny=<n> option will deny access if the number of consecutive authentication failures for this user during the recent interval exceeds
.
Locking out user IDs after
n
unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

### Solution

Create or edit the following line in /etc/security/faillock.conf setting the deny option to 5 or less:
deny = 5
Run the following command:
# grep -Pl -- 'bpam_faillock.soh+([^# r]+h+)?denyb' /usr/share/pam-configs/*
Edit any returned files and remove the deny=<N> arguments from the pam_faillock.so line(s):

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171R3** | 03.01.01 |
| **800-171R3** | 03.15.01 |
| **800-53** | AC-1 |
| **800-53** | AC-2 |
| **800-53** | AC-2(1) |
| **800-53R5** | AC-1 |
| **800-53R5** | AC-2 |
| **800-53R5** | AC-2(1) |
| **CN-L3** | 7.1.3.2(d) |
| **CN-L3** | 8.1.4.2(e) |
| **CN-L3** | 8.1.10.6(c) |
| **CSCV7** | 16.7 |
| **CSCV8** | 6.2 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | ID.GV-1 |
| **CSF** | ID.GV-3 |
| **CSF** | PR.AC-1 |
| **CSF** | PR.AC-4 |
| **CSF2.0** | DE.CM-01 |

| | |
|---|---|
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | GV.OC-03 |
| **CSF2.0** | GV.OV-01 |
| **CSF2.0** | GV.PO-01 |
| **CSF2.0** | GV.PO-02 |
| **CSF2.0** | GV.SC-03 |
| **CSF2.0** | ID.IM-01 |
| **CSF2.0** | ID.IM-02 |
| **CSF2.0** | ID.IM-03 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.1 |
| **ISO-27001-2022** | A.5.2 |
| **ISO-27001-2022** | A.5.4 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.18 |
| **ISO-27001-2022** | A.5.31 |
| **ISO-27001-2022** | A.5.36 |
| **ISO-27001-2022** | A.5.37 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | 5.2 |
| **ISO-27001-2022** | 5.3 |
| **ISO-27001-2022** | 7.5.1 |
| **ISO-27001-2022** | 7.5.2 |
| **ISO-27001-2022** | 7.5.3 |
| **ISO/IEC-27001** | A.9.1.1 |

| | |
|---|---|
| **ISO/IEC-27001** | A.9.2.1 |
| **ITSG-33** | AC-1 |
| **ITSG-33** | AC-2 |
| **ITSG-33** | AC-2(1) |
| **LEVEL** | 1A |
| **NESA** | M1.2.2 |
| **NIAV2** | AM28 |
| **NIAV2** | AM29 |
| **NIAV2** | AM30 |
| **NIAV2** | NS5j |
| **NIAV2** | SS14e |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 13.2 |
| **QCSC-V1** | 15.2 |

### Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - /etc/security/faillock.conf
The following file(s) do not contain "(?i)^\h*deny\h*=\h*[1-5]\b":
      /etc/security/faillock.conf

-------------------------
PASSED - /etc/pam.d/common-auth
No matching files were found
```

## 5.3.3.1.2 Ensure password unlock time is configured

### Info

unlock_time=<n> - The access will be re-enabled after
seconds after the lock out. The value 0 has the same meaning as value never - the access will not be re-enabled without resetting the faillock entries by the faillock(8) command.
Note:
- The default directory that pam_faillock uses is usually cleared on system boot so the access will be also re-enabled after system reboot. If that is undesirable a different tally directory must be set with the dir option.
- It is usually undesirable to permanently lock out users as they can become easily a target of denial of service attack unless the usernames are random and kept secret to potential attackers.
- The maximum configurable value for unlock_time is 604800
Locking out user IDs after
n
unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

### Solution

Set password unlock time to conform to site policy. unlock_time should be 0 (never), or 900 seconds or greater.
Edit /etc/security/faillock.conf and update or add the following line:
unlock_time = 900
Run the following command: remove the unlock_time argument from the pam_faillock.so module in the PAM files:
# grep -Pl -- 'bpam_faillock.soh+([^# r]+h+)?unlock_timeb' /usr/share/pam-configs/*
Edit any returned files and remove the unlock_time=<N> argument from the pam_faillock.so line(s):
Impact:
Use of unlock_time=0 may allow an attacker to cause denial of service to legitimate users. This will also require a systems administrator with elevated privileges to unlock the account.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171R3** | 03.01.01 |
| **800-171R3** | 03.15.01 |
| **800-53** | AC-1 |
| **800-53** | AC-2 |
| **800-53** | AC-2(1) |
| **800-53R5** | AC-1 |
| **800-53R5** | AC-2 |
| **800-53R5** | AC-2(1) |
| **CN-L3** | 7.1.3.2(d) |
| **CN-L3** | 8.1.4.2(e) |
| **CN-L3** | 8.1.10.6(c) |
| **CSCV7** | 16.7 |
| **CSCV8** | 6.2 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |

| | |
|---|---|
| **CSF** | ID.GV-1 |
| **CSF** | ID.GV-3 |
| **CSF** | PR.AC-1 |
| **CSF** | PR.AC-4 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | GV.OC-03 |
| **CSF2.0** | GV.OV-01 |
| **CSF2.0** | GV.PO-01 |
| **CSF2.0** | GV.PO-02 |
| **CSF2.0** | GV.SC-03 |
| **CSF2.0** | ID.IM-01 |
| **CSF2.0** | ID.IM-02 |
| **CSF2.0** | ID.IM-03 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.1 |
| **ISO-27001-2022** | A.5.2 |
| **ISO-27001-2022** | A.5.4 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.18 |
| **ISO-27001-2022** | A.5.31 |
| **ISO-27001-2022** | A.5.36 |
| **ISO-27001-2022** | A.5.37 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | 5.2 |

| | |
|---|---|
| **ISO-27001-2022** | 5.3 |
| **ISO-27001-2022** | 7.5.1 |
| **ISO-27001-2022** | 7.5.2 |
| **ISO-27001-2022** | 7.5.3 |
| **ISO/IEC-27001** | A.9.1.1 |
| **ISO/IEC-27001** | A.9.2.1 |
| **ITSG-33** | AC-1 |
| **ITSG-33** | AC-2 |
| **ITSG-33** | AC-2(1) |
| **LEVEL** | 1A |
| **NESA** | M1.2.2 |
| **NIAV2** | AM28 |
| **NIAV2** | AM29 |
| **NIAV2** | AM30 |
| **NIAV2** | NS5j |
| **NIAV2** | SS14e |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 13.2 |
| **QCSC-V1** | 15.2 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - /etc/security/faillock.conf
The following file(s) do not contain "(?i)^\h*unlock_time\h*=":
      /etc/security/faillock.conf

-------------------------
PASSED - /etc/pam.d/common-auth
No matching files were found
```

## 5.3.3.2.1 Ensure password number of changed characters is configured

### Info

The pwquality difok option sets the number of characters in a password that must not be present in the old password.
Use of a complex password helps to increase the time and resources required to compromise the password.
Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.
Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

### Solution

Create or modify a file ending inconf in the /etc/security/pwquality.conf.d/ directory or the file /etc/security/pwquality.conf and add or modify the following line to set difok to 2 or more. Ensure setting conforms to local site policy:
Example:

```
#!/usr/bin/env bash
{ sed -ri 's/^s*difoks*=/# &/' /etc/security/pwquality.conf [ ! -d /etc/security/pwquality.conf.d/ ] && mkdir /etc/security/
pwquality.conf.d/ printf '
%s' "difok = 2" > /etc/security/pwquality.conf.d/50-pwdifok.conf }
```

Run the following command:

```
# grep -Pl -- 'bpam_pwquality.soh+([^# r]+h+)?difokb' /usr/share/pam-configs/*
```

Edit any returned files and remove the difok argument from the pam_pwquality.so line(s):

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |

|  |  |
|---|---|
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - pwquality - difok
No files found: /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf

-------------------------
PASSED - /etc/pam.d/common-password
No matching files were found
```

## 5.3.3.2.2 Ensure minimum password length is configured

### Info

The minimum password length setting determines the lowers number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "passphrase" is a better term than "password".
The minlen option sets the minimum acceptable size for the new password (plus one if credits are not disabled which is the default). Cannot be set to lower value than 6.
Strong passwords help protect systems from password attacks. Types of password attacks include dictionary attacks, which attempt to use common words and phrases, and brute force attacks, which try every possible combination of characters. Also attackers may try to obtain the account database so they can use tools to discover the accounts and passwords.

### Solution

Create or modify a file ending inconf in the /etc/security/pwquality.conf.d/ directory or the file /etc/security/pwquality.conf and add or modify the following line to set password length of 14 or more characters. Ensure that password length conforms to local site policy:
Example:

```
#!/usr/bin/env bash
{ sed -ri 's/^s*minlens*=/# &/' /etc/security/pwquality.conf [ ! -d /etc/security/pwquality.conf.d/ ] && mkdir /etc/security/
pwquality.conf.d/ printf '
%s' "minlen = 14" > /etc/security/pwquality.conf.d/50-pwlength.conf }
```

Run the following command:

```
# grep -Pl -- 'bpam_pwquality.soh+([^# r]+h+)?minlenb' /usr/share/pam-configs/*
```

Edit any returned files and remove the minlen argument from the pam_pwquality.so line(s):
Impact:
In general, it is true that longer passwords are better (harder to crack), but it is also true that forced password length requirements can cause user behavior that is predictable and undesirable. For example, requiring users to have a minimum 16-character password may cause them to choose repeating patterns like fourfourfourfour or passwordpassword that meet the requirement but aren't hard to guess. Additionally, length requirements increase the chances that users will adopt other insecure practices, like writing them down, re-using them or storing them unencrypted in their documents.
Having a reasonable minimum length with no maximum character limit increases the resultingaverage password length used (and therefore the strength).6

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |

| | |
|---|---|
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - /etc/pam.d/common-password
No matching files were found

-------------------------
FAILED - pwquality - minlen
No files found: /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf
```

## 5.3.3.2.3 Ensure password complexity is configured

### Info

Password complexity can be set through:
- minclass - The minimum number of classes of characters required in a new password. (digits, uppercase, lowercase, others). e.g. minclass = 4 requires digits, uppercase, lower case, and special characters.
- dcredit - The maximum credit for having digits in the new password. If less than 0 it is the minimum number of digits in the new password. e.g. dcredit = -1 requires at least one digit
- ucredit - The maximum credit for having uppercase characters in the new password. If less than 0 it is the minimum number of uppercase characters in the new password. e.g. ucredit = -1 requires at least one uppercase character
- ocredit - The maximum credit for having other characters in the new password. If less than 0 it is the minimum number of other characters in the new password. e.g. ocredit = -1 requires at least one special character
- lcredit - The maximum credit for having lowercase characters in the new password. If less than 0 it is the minimum number of lowercase characters in the new password. e.g. lcredit = -1 requires at least one lowercase character
Strong passwords protect systems from being hacked through brute force methods.
Requiring at least one non-alphabetic character increases the search space beyond pure dictionary words, which makes the resulting password harder to crack.
Forcing users to choose an excessively complex password, e.g. some combination of upper-case, lower-case, numbers, and special characters, has a negative impact. It places an extra burden on users and many will use predictable patterns (for example, a capital letter in the first position, followed by lowercase letters, then one or two numbers, and a "special character" at the end). Attackers know this, so dictionary attacks will often contain these common patterns and use the most common substitutions like, $ for s, @ for a, 1 for l, 0 for o.

### Solution

Run the following command:
# grep -Pl -- 'bpam_pwquality.soh+([^# r]+h+)?(minclass|[dulo]credit)b' /usr/share/pam-configs/*
Edit any returned files and remove the minclass dcredit ucredit lcredit and ocredit arguments from the pam_pwquality.so line(s)
Create or modify a file ending inconf in the /etc/security/pwquality.conf.d/ directory or the file /etc/security/pwquality.conf and add or modify the following line(s) to set complexity according to local site policy:
- minclass = _N_
- dcredit = _N_ # Value should be either 0 or a number proceeded by a minus ( - ) symbol
- ucredit = -1 # Value should be either 0 or a number proceeded by a minus ( - ) symbol
- ocredit = -1 # Value should be either 0 or a number proceeded by a minus ( - ) symbol
- lcredit = -1 # Value should be either 0 or a number proceeded by a minus ( - ) symbol
Example 1 - Set minclass = 3 :
#!/usr/bin/env bash
{ sed -ri 's/^s*minclasss*=/# &/' /etc/security/pwquality.conf sed -ri 's/^s*[dulo]credits*=/# &/' /etc/security/pwquality.conf [ ! -d /etc/security/pwquality.conf.d/ ] && mkdir /etc/security/pwquality.conf.d/ printf '
%s' "minclass = 3" > /etc/security/pwquality.conf.d/50-pwcomplexity.conf }
Example 2 - set dcredit = -1 ucredit = -1 and lcredit = -1 :
#!/usr/bin/env bash
{ sed -ri 's/^s*minclasss*=/# &/' /etc/security/pwquality.conf sed -ri 's/^s*[dulo]credits*=/# &/' /etc/security/pwquality.conf [ ! -d /etc/security/pwquality.conf.d/ ] && mkdir /etc/security/pwquality.conf.d/ printf '%s ' "dcredit = -1" "ucredit = -1" "lcredit = -1" > /etc/security/pwquality.conf.d/50-pwcomplexity.conf }
Impact:
Passwords that are too complex in nature make it harder for users to remember, leading to bad practices. In addition, composition requirements provide no defense against common attack types such as social engineering or insecure storage of passwords

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |

| | |
|---|---|
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1M |
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - ocredit
No files found: /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf

-------------------------
FAILED - ucredit
No files found: /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf

-------------------------
FAILED - lcredit
No files found: /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf

-------------------------
FAILED - dcredit
No files found: /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf
```

## 5.3.3.2.4 Ensure password same consecutive characters is configured

### Info

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

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

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

### Solution

Create or modify a file ending inconf in the /etc/security/pwquality.conf.d/ directory or the file /etc/security/pwquality.conf and add or modify the following line to set maxrepeat to 3 or less and not 0 Ensure setting conforms to local site policy:

Example:

```
#!/usr/bin/env bash
{ sed -ri 's/^s*maxrepeats*=/# &/' /etc/security/pwquality.conf [ ! -d /etc/security/pwquality.conf.d/ ] && mkdir /etc/
security/pwquality.conf.d/ printf '
%s' "maxrepeat = 3" > /etc/security/pwquality.conf.d/50-pwrepeat.conf }
```

Run the following command:

```
# grep -Pl -- 'bpam_pwquality.soh+([^# r]+h+)?maxrepeatb' /usr/share/pam-configs/*
```

Edit any returned files and remove the maxrepeat argument from the pam_pwquality.so line(s):

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |

|  |  |
|---|---|
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - pwquality - maxrepeat
No files found: /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf

-------------------------
PASSED - /etc/pam.d/common-password
No matching files were found
```

## 5.3.3.2.5 Ensure password maximum sequential characters is configured

### Info

The pwquality maxsequence option sets the maximum length of monotonic character sequences in the new password. Examples of such sequence are 12345 or fedcb The check is disabled if the value is 0
Note: Most such passwords will not pass the simplicity check unless the sequence is only a minor part of the password.
Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.
Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

### Solution

Create or modify a file ending inconf in the /etc/security/pwquality.conf.d/ directory or the file /etc/security/pwquality.conf and add or modify the following line to set maxsequence to 3 or less and not 0 Ensure setting conforms to local site policy:
Example:

```
#!/usr/bin/env bash
{ sed -ri 's/^s*maxsequences*=/# &/' /etc/security/pwquality.conf [ ! -d /etc/security/pwquality.conf.d/ ] && mkdir /etc/
security/pwquality.conf.d/ printf '
%s' "maxsequence = 3" > /etc/security/pwquality.conf.d/50-pwmaxsequence.conf }
```

Run the following command:

```
# grep -Pl -- 'bpam_pwquality.soh+([^# r]+h+)?maxsequenceb' /usr/share/pam-configs/*
```

Edit any returned files and remove the maxsequence argument from the pam_pwquality.so line(s):

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |

|  |  |
|---|---|
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - pwquality - maxsequence
No files found: /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf

-------------------------
PASSED - /etc/pam.d/common-password
No matching files were found
```

## 5.3.3.2.6 Ensure password dictionary check is enabled

### Info

The pwquality dictcheck option sets whether to check for the words from the cracklib dictionary.
If the operating system allows the user to select passwords based on dictionary words, this increases the chances of password compromise by increasing the opportunity for successful guesses, and brute-force attacks.

### Solution

Edit any file ending inconf in the /etc/security/pwquality.conf.d/ directory and/or the file /etc/security/pwquality.conf and comment out or remove any instance of dictcheck = 0 :
Example:

```
# sed -ri 's/^s*dictchecks*=/# &/' /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf
```

Run the following command:

```
# grep -Pl -- 'bpam_pwquality.soh+([^# r]+h+)?dictcheckb' /usr/share/pam-configs/*
```

Edit any returned files and remove the dictcheck argument from the pam_pwquality.so line(s)

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

### Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - pwquality - dictcheck
No files found: /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf

-------------------------
PASSED - /etc/pam.d/common-password
The following file(s) do not contain "(?i)^\h*password\h+(requisite|required|sufficient)\h
+pam_pwquality\.so\h+([^#\r]+\h+)?dictcheck\h*=\h*0\b":
      /etc/pam.d/common-password
```

## 5.3.3.2.7 Ensure password quality checking is enforced

### Info

The pam_pwquality module can be configured to either reject a password if it fails the checks, or only print a warning. This is configured by setting the enforcing=<N> argument. If nonzero, a password will be rejected if it fails the checks, otherwise only a warning message will be provided.

This setting applies only to the pam_pwquality module and possibly other applications that explicitly change their behavior based on it. It does not affect pwmake(1) and pwscore(1).

Strong passwords help protect systems from password attacks. Types of password attacks include dictionary attacks, which attempt to use common words and phrases, and brute force attacks, which try every possible combination of characters. Also attackers may try to obtain the account database so they can use tools to discover the accounts and passwords.

### Solution

Run the following command:

```
# grep -Pl -- 'bpam_pwquality.soh+([^# r]+h+)?enforcing=0b' /usr/share/pam-configs/*
```

Edit any returned files and remove the enforcing=0 argument from the pam_pwquality.so line(s)

Edit /etc/security/pwquality.conf and all files ending inconf in the /etc/security/pwquality.conf.d/ directory and remove or comment out any line containing the enforcing = 0 argument:

Example:

```
# sed -ri 's/^s*enforcings*=s*0/# &/' /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |

| | |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - /etc/pam.d/common-password
The following file(s) do not contain "(?i)^\h*password\h+(requisite|required|sufficient)\h
+pam_pwquality\.so\h+([^#\r]+\h+)?enforcing\h*=\h*0\b":
      /etc/pam.d/common-password

-------------------------
FAILED - pwquality - enforcing
No files found: /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf
```

## 5.3.3.2.8 Ensure password quality is enforced for the root user

### Info

If the pwquality enforce_for_root option is enabled, the module will return error on failed check even if the user changing the password is root.
This option is off by default which means that just the message about the failed check is printed but root can change the password anyway.
Note: The root is not asked for an old password so the checks that compare the old and new password are not performed.
Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.
Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

### Solution

Edit or add the following line in a *.conf file in /etc/security/pwquality.conf.d or in /etc/security/pwquality.conf :
Example:
#!/urs/bin/env bash
{ [ ! -d /etc/security/pwquality.conf.d/ ] && mkdir /etc/security/pwquality.conf.d/ printf '
%s ' "enforce_for_root" > /etc/security/pwquality.conf.d/50-pwroot.conf }

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |

|  |  |
|---|---|
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

### Assets

#### linux_project

```
No files found: /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf
```

## 5.3.3.3.1 Ensure password history remember is configured

### Info

The /etc/security/opasswd file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords. The number of passwords remembered is set via the remember argument value in set for the pam_pwhistory module.

- remember=<N> - <N> is the number of old passwords to remember

Requiring users not to reuse their passwords make it less likely that an attacker will be able to guess the password or use a compromised password.

Note: These change only apply to accounts configured on the local system.

### Solution

Run the following command:

```
# awk '/Password-Type:/{ f = 1;next } /-Type:/{ f = 0 } f {if (/pam_pwhistory.so/) print FILENAME}' /usr/share/pam-configs/*
```

Edit any returned files and edit or add the remember= argument, with a value of 24 or more, that meets local site policy to the pam_pwhistory line in the Password section:

Example File:

Name: pwhistory password history checking Default: yes Priority: 1024 Password-Type: Primary Password: requisite pam_pwhistory.so remember=24 enforce_for_root try_first_pass use_authtok # <- **ensure line includes remember=<N>**

Run the following command to update the files in the /etc/pam.d/ directory:

```
# pam-auth-update --enable <MODIFIED_PROFILE_NAME>
```

Example:

```
# pam-auth-update --enable pwhistory
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |

|  |  |
|---|---|
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

## Assets

### linux_project

```
The following file(s) do not contain "(?i)^\h*password\h+(requisite|required|sufficient)\h
+pam_pwhistory\.so\h+([^#\r]+\h+)?remember=":
      /etc/pam.d/common-password
```

## 5.3.3.3.2 Ensure password history is enforced for the root user

### Info

If the pwhistory enforce_for_root option is enabled, the module will enforce password history for the root user as well
Requiring users not to reuse their passwords make it less likely that an attacker will be able to guess the password or use a compromised password
Note: These change only apply to accounts configured on the local system.

### Solution

Run the following command:

```
# awk '/Password-Type:/{ f = 1;next } /-Type:/{ f = 0 } f {if (/pam_pwhistory.so/) print FILENAME}' /usr/share/pam-configs/*
```

Edit any returned files and add the enforce_for_root argument to the pam_pwhistory line in the Password section:
Example File:
Name: pwhistory password history checking Default: yes Priority: 1024 Password-Type: Primary Password: requisite pam_pwhistory.so remember=24 enforce_for_root try_first_pass use_authtok # <- **ensure line includes enforce_for_root**
Run the following command to update the files in the /etc/pam.d/ directory:

```
# pam-auth-update --enable <MODIFIED_PROFILE_NAME>
```

Example:

```
# pam-auth-update --enable pwhistory
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |

| | |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

## Assets

### linux_project

```
The following file(s) do not contain "(?i)^\h*password\h+[^#\n\r]+\h+pam_pwhistory\.so\h+([^#\n
\r]+\h+)?enforce_for_root\b":
      /etc/pam.d/common-password
```

## 5.3.3.3.3 Ensure pam_pwhistory includes use_authtok

### Info

use_authtok - When password changing enforce the module to set the new password to the one provided by a previously stacked password module
use_authtok allows multiple pam modules to confirm a new password before it is accepted.

### Solution

Run the following command:

```
# awk '/Password-Type:/{ f = 1;next } /-Type:/{ f = 0 } f {if (/pam_pwhistory.so/) print FILENAME}' /usr/share/pam-configs/*
```

Edit any returned files and add the use_authtok argument to the pam_pwhistory line in the Password section:
Example File:

```
Name: pwhistory password history checking Default: yes Priority: 1024 Password-Type: Primary Password: requisite pam_pwhistory.so remember=24 enforce_for_root try_first_pass use_authtok # <- **ensure line includes use_authtok**
```

Run the following command to update the files in the /etc/pam.d/ directory:

```
# pam-auth-update --enable <MODIFIED_PROFILE_NAME>
```

Example:

```
# pam-auth-update --enable pwhistory
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171** | 3.13.16 |
| **800-171R3** | 03.05.07 |
| **800-171R3** | 03.13.08 |
| **800-53** | IA-5(1) |
| **800-53** | SC-28 |
| **800-53** | SC-28(1) |
| **800-53R5** | IA-5(1) |
| **800-53R5** | SC-28 |
| **800-53R5** | SC-28(1) |
| **CN-L3** | 8.1.4.7(b) |
| **CN-L3** | 8.1.4.8(b) |
| **CSCV7** | 16.4 |
| **CSCV8** | 3.11 |
| **CSF** | PR.AC-1 |
| **CSF** | PR.DS-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **CSF2.0** | PR.DS-01 |

| | |
|---|---|
| **GDPR** | 32.1.a |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(a)(2)(iv) |
| **HIPAA** | 164.312(d) |
| **HIPAA** | 164.312(e)(2)(ii) |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ISO-27001-2022** | A.5.33 |
| **ITSG-33** | IA-5(1) |
| **ITSG-33** | SC-28 |
| **ITSG-33** | SC-28a. |
| **ITSG-33** | SC-28(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **PCI-DSSV3.2.1** | 3.4 |
| **PCI-DSSV4.0** | 3.3.2 |
| **PCI-DSSV4.0** | 3.5.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |
| **TBA-FIISB** | 28.1 |

### Assets

### linux_project

```
The following file(s) do not contain "(?i)^\h*password\h+(requisite|required|sufficient)\h
+pam_pwhistory\.so(\h+[^#\n\r]+)?\h+use_authtok\b":
      /etc/pam.d/common-password
```

## 5.3.3.4.1 Ensure pam_unix does not include nullok

### Info

The nullok argument overrides the default action of pam_unix.so to not permit the user access to a service if their official password is blank.
Using a strong password is essential to helping protect personal and sensitive information from unauthorized access

### Solution

Run the following command:
# grep -PH -- '^h*([^# r]+h+)?pam_unix.soh+([^# r]+h+)?nullokb' /usr/share/pam-configs/*
Edit any files returned and remove the nullok argument for the pam_unix lines
Example File:
Name: Unix authentication Default: yes Priority: 256 Auth-Type: Primary Auth:
[success=end default=ignore] pam_unix.so try_first_pass # <- **ensure line does not include nullok nullok** Auth-Initial:
[success=end default=ignore] pam_unix.so # <- **ensure line does not include nullok nullok** Account-Type: Primary Account:
[success=end new_authtok_reqd=done default=ignore] pam_unix.so Account-Initial:
[success=end new_authtok_reqd=done default=ignore] pam_unix.so Session-Type: Additional Session:
required pam_unix.so Session-Initial:
required pam_unix.so Password-Type: Primary Password:
[success=end default=ignore] pam_unix.so obscure use_authtok try_first_pass yescrypt Password-Initial:
[success=end default=ignore] pam_unix.so obscure yescrypt
Run the following command to update the files in the /etc/pam.d/ directory:
# pam-auth-update --enable <EDITED_PROFILE_NAME>
Example:
# pam-auth-update --enable unix
Note: If custom files are being used, the corresponding files in /etc/pam.d/ would need to be edited directly, and the pam-auth-update --enable <EDITED_PROFILE_NAME> command skipped

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |

| | |
|---|---|
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - /etc/pamd./common-session-noninteractive nullok
The following file(s) do not contain "(?i)^\h*^\h*[^#\n\r]+\h+pam_unix\.so\b[^#\n\r]+nullok\b":
      /etc/pam.d/common-session-noninteractive

-------------------------
PASSED - /etc/pamd./common-password nullok
The following file(s) do not contain "(?i)^\h*^\h*[^#\n\r]+\h+pam_unix\.so\b[^#\n\r]+nullok\b":
      /etc/pam.d/common-password

-------------------------
FAILED - /etc/pamd./common-auth nullok
Non-compliant file(s):
      /etc/pam.d/common-auth - regex '(?i)^\h*^\h*[^#\n\r]+\h+pam_unix\.so\b[^#\n\r]+nullok\b'
 found - expect '(?i)^\h*^\h*[^#\n\r]+\h+pam_unix\.so\b[^#\n\r]+nullok\b' found in the following
 lines:
          17: auth [success=1 default=ignore] pam_unix.so nullok

-------------------------
PASSED - /etc/pamd./common-account nullok
The following file(s) do not contain "(?i)^\h*^\h*[^#\n\r]+\h+pam_unix\.so\b[^#\n\r]+nullok\b":
      /etc/pam.d/common-account

-------------------------
PASSED - /etc/pamd./common-session nullok
The following file(s) do not contain "(?i)^\h*^\h*[^#\n\r]+\h+pam_unix\.so\b[^#\n\r]+nullok\b":
      /etc/pam.d/common-session
```

## 5.3.3.4.4 Ensure pam_unix includes use_authtok

### Info

use_authtok - When password changing enforce the module to set the new password to the one provided by a previously stacked password module

use_authtok allows multiple pam modules to confirm a new password before it is accepted.

### Solution

Run the following command:

```
# awk '/Password-Type:/{ f = 1;next } /-Type:/{ f = 0 } f {if (/pam_unix.so/) print FILENAME}' /usr/share/pam-configs/*
```

Edit any returned files add use_authtok to the pam_unix line in the Password section under Password: subsection:

Note: The if the file's Password section includes a Password-Initial: subsection, use_authtok should not be added to the pam_unix line in the Password-Initial: subsection

Example File:

Name: Unix authentication Default: yes Priority: 256 Auth-Type: Primary # <- Start of "Auth" section Auth:

[success=end default=ignore] pam_unix.so try_first_pass Auth-Initial:

[success=end default=ignore] pam_unix.so Account-Type: Primary # <- Start of "Account" section Account:

[success=end new_authtok_reqd=done default=ignore] pam_unix.so Account-Initial:

[success=end new_authtok_reqd=done default=ignore] pam_unix.so Session-Type: Additional # <- Start of "Session" section Session:

required pam_unix.so Session-Initial:

required pam_unix.so Password-Type: Primary # <- Start of "Password" section Password:

[success=end default=ignore] pam_unix.so obscure use_authtok try_first_pass yescrypt # <- **ensure line includes use_authtok** Password-Initial:

[success=end default=ignore] pam_unix.so obscure yescrypt # <- **Password-Initial: subsection does not include use_authtok

Run the following command to update the files in the /etc/pam.d/ directory:

```
# pam-auth-update --enable <MODIFIED_PROFILE_NAME>
```

Example:

```
# pam-auth-update --enable unix
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171** | 3.13.16 |
| **800-171R3** | 03.05.07 |
| **800-171R3** | 03.13.08 |
| **800-53** | IA-5(1) |
| **800-53** | SC-28 |
| **800-53** | SC-28(1) |
| **800-53R5** | IA-5(1) |
| **800-53R5** | SC-28 |
| **800-53R5** | SC-28(1) |
| **CN-L3** | 8.1.4.7(b) |
| **CN-L3** | 8.1.4.8(b) |
| **CSCV7** | 16.4 |
| **CSCV8** | 3.11 |

| | |
|---|---|
| **CSF** | PR.AC-1 |
| **CSF** | PR.DS-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **CSF2.0** | PR.DS-01 |
| **GDPR** | 32.1.a |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(a)(2)(iv) |
| **HIPAA** | 164.312(d) |
| **HIPAA** | 164.312(e)(2)(ii) |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ISO-27001-2022** | A.5.33 |
| **ITSG-33** | IA-5(1) |
| **ITSG-33** | SC-28 |
| **ITSG-33** | SC-28a. |
| **ITSG-33** | SC-28(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **PCI-DSSV3.2.1** | 3.4 |
| **PCI-DSSV4.0** | 3.3.2 |
| **PCI-DSSV4.0** | 3.5.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |
| **TBA-FIISB** | 28.1 |

| Assets |
|---|
| **linux_project** |

```
The following file(s) do not contain "(?i)^\h*password\h+([^#\n\r]+)\h+pam_unix\.so\h+([^#\n\r]+\h
+)?use_authtok\b":
      /etc/pam.d/common-password
```

## 5.4.1.1 Ensure password expiration is configured

### Info

The PASS_MAX_DAYS parameter in /etc/login.defs allows an administrator to force passwords to expire once they reach a defined age.
PASS_MAX_DAYS
<N>
- The maximum number of days a password may be used. If the password is older than this, a password change will be forced. If not specified, -1 will be assumed (which disables the restriction).
The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity.
We recommend a yearly password change. This is primarily because for all their good intentions users will share credentials across accounts. Therefore, even if a breach is publicly identified, the user may not see this notification, or forget they have an account on that site. This could leave a shared credential vulnerable indefinitely. Having an organizational policy of a 1-year (annual) password expiration is a reasonable compromise to mitigate this with minimal user burden.

### Solution

Set the PASS_MAX_DAYS parameter to conform to site policy in /etc/login.defs :
PASS_MAX_DAYS 365
Modify user parameters for all users with a password set to match:
# chage --maxdays 365 <user>
Edit /etc/login.defs and set PASS_MAX_DAYS to a value greater than 0 that follows local site policy:
Example:
PASS_MAX_DAYS 365
Run the following command to modify user parameters for all users with a password set to a maximum age no greater than 365 or less than 1 that follows local site policy:
# chage --maxdays <N> <user>
Example:
# awk -F: '($2~/^$.+$/) {if($5 > 365 || $5 < 1)system ("chage --maxdays 365 " $1)}' /etc/shadow
Warning: If a password has been set at system install or kickstart, the last change date field is not set, In this case, setting PASS_MAX_DAYS will immediately expire the password. One possible solution is to populate the last change date field through a command like: chage -d "$(date +%Y-%m-%d)" root
Impact:
The password expiration must be greater than the minimum days between password changes or users will be unable to change their password.
Excessive password expiration requirements do more harm than good, because these requirements make users select predictable passwords, composed of sequential words and numbers that are closely related to each other. In these cases, the next password can be predicted based on the previous one (incrementing a number used in the password forexample). Also, password expiration requirements offer no containment benefits because attackers will often use credentials as soon as they compromise them. Instead, immediate password changes should be based on key events including, but not limited to:
- Indication of compromise
- Change of user roles
- When a user leaves the organization.
Not only does changing passwords every few weeks or months frustrate the user, but it's also been suggested that it does more harm than good, because it could lead to bad practices by the user such as adding a character to the end of their existing password.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |

| | |
|---|---|
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - login.defs - PASSWORD_MAX_DAYS
Non-compliant file(s):
      /etc/login.defs - regex '(?i)^\h*PASS_MAX_DAYS\h+\d+\b' found - expect '(?i)^
\h*PASS_MAX_DAYS\h+365\b' not found in the following lines:
          165: PASS_MAX_DAYS 99999

-------------------------
FAILED - shadow password max days
The command '/bin/awk -F: '($2~/^\$.+\$/) {if($5 > 365 || $5 < 1)print "User: " $1 "
 PASS_MAX_DAYS: " $5}' /etc/shadow | /bin/awk '{print} END {if (NR == 0) print "pass"; else print
 "fail"}'' returned :

User: root PASS_MAX_DAYS: 99999
fail
```

## 5.4.1.5 Ensure inactive password lock is configured

### Info

User accounts that have been inactive for over a given period of time can be automatically disabled.
INACTIVE - Defines the number of days after the password exceeded its maximum age where the user is expected to replace this password.
The value is stored in the shadow password file. An input of 0 will disable an expired password with no delay. An input of -1 will blank the respective field in the shadow password file.
Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

### Solution

Run the following command to set the default password inactivity period to 45 days or less that meets local site policy:
# useradd -D -f <N>
Example:
# useradd -D -f 45
Run the following command to modify user parameters for all users with a password set to a inactive age of 45 days or less that follows local site policy:
# chage --inactive <N> <user>
Example:
# awk -F: '($2~/^$.+$/) {if($7 > 45 || $7 < 0)system ("chage --inactive 45 " $1)}' /etc/shadow

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |

| | |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - shadow password inactive days
The command '/bin/awk -F: '($2~/^\$.+\$/) {if($7 > 45 || $7 < 0)print "User: " $1 " INACTIVE:
 " $7}' /etc/shadow | /bin/awk '{print} END {if (NR == 0) print "pass"; else print "fail"}''
 returned :

User: root INACTIVE:
fail

-------------------------
FAILED - useradd - INACTIVE
The command '/sbin/useradd -D | /bin/grep 'INACTIVE'' returned :

INACTIVE=-1
```

## 5.4.2.5 Ensure root path integrity

### Info

The root user can execute any command on the system and could be fooled into executing programs unintentionally if the PATH is not set correctly.
Including the current working directory (.) or other writable directory in root 's executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as root to execute a Trojan horse program.

### Solution

Correct or justify any:
- Locations that are not directories
- Empty directories ( :: )
- Trailing ( : )
- Current working directory ( )
- Non root owned directories
- Directories that less restrictive than mode 0755

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-7(2) |
| **800-53R5** | CM-7(2) |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ITSG-33** | CM-7(2) |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **QCSC-V1** | 3.2 |
| **SWIFT-CSCV1** | 2.3 |

### Assets

#### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - * Reasons for audit failure * :

 - "/snap/bin" is not a directory
```

## 5.4.3.2 Ensure default user shell timeout is configured

### Info

TMOUT is an environmental setting that determines the timeout of a shell in seconds.
- TMOUT=
n
- Sets the shell timeout to
n
seconds. A setting of TMOUT=0 disables timeout.
- readonly TMOUT- Sets the TMOUT environmental variable as readonly, preventing unwanted modification during run-time.
- export TMOUT - exports the TMOUT variable
System Wide Shell Configuration Files:
- /etc/profile - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in thebash_profile however this file is used to set an initial PATH or PS1 for all shell users of the system. is only executed for interactive
login
shells, or shells executed with the --login parameter.
- /etc/profile.d - /etc/profile will execute the scripts within /etc/profile.d/*.sh It is recommended to place your configuration in a shell script within /etc/profile.d to set your own system wide environmental variables.
- /etc/bashrc - System wide version ofbashrc In Fedora derived distributions, /etc/bashrc also invokes /etc/profile.d/*.sh if
non-login
shell, but redirects output to /dev/null if
non-interactive.
Is only executed for
interactive
shells or if BASH_ENV is set to /etc/bashrc
Setting a timeout value reduces the window of opportunity for unauthorized user access to another user's shell session that has been left unattended. It also ends the inactive session and releases the resources associated with that session.

### Solution

Review /etc/bashrc /etc/profile and all files ending in *.sh in the /etc/profile.d/ directory and remove or edit all TMOUT=_n_ entries to follow local site policy. TMOUT should not exceed 900 or be equal to 0
Configure TMOUT in one of the following files:
- A file in the /etc/profile.d/ directory ending insh
- /etc/profile
- /etc/bashrc
TMOUT configuration examples:
- As multiple lines:
TMOUT=900 readonly TMOUT export TMOUT
- As a single line:
readonly TMOUT=900 ; export TMOUT

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.10 |
| **800-171** | 3.1.11 |
| **800-171R3** | 03.01.01h. |
| **800-171R3** | 03.01.10 |
| **800-171R3** | 03.01.11 |
| **800-53** | AC-2(5) |
| **800-53** | AC-11 |

| | |
|---|---|
| **800-53** | AC-11(1) |
| **800-53** | AC-12 |
| **800-53R5** | AC-2(5) |
| **800-53R5** | AC-11 |
| **800-53R5** | AC-11(1) |
| **800-53R5** | AC-12 |
| **CN-L3** | 7.1.2.2(d) |
| **CN-L3** | 7.1.3.2(d) |
| **CN-L3** | 7.1.3.7(b) |
| **CN-L3** | 8.1.4.1(b) |
| **CSCV7** | 16.11 |
| **CSCV8** | 4.3 |
| **CSF** | PR.AC-1 |
| **CSF** | PR.AC-4 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **HIPAA** | 164.312(a)(2)(iii) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.18 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.8.1 |
| **ISO-27001-2022** | A.8.2 |
| **ISO/IEC-27001** | A.9.2.1 |
| **ISO/IEC-27001** | A.11.2.8 |

| | |
|---|---|
| **ITSG-33** | AC-2(5) |
| **ITSG-33** | AC-11 |
| **ITSG-33** | AC-11(1) |
| **ITSG-33** | AC-12 |
| **LEVEL** | 1A |
| **NIAV2** | AM23c |
| **NIAV2** | AM23d |
| **NIAV2** | AM28 |
| **NIAV2** | NS5j |
| **NIAV2** | NS49 |
| **NIAV2** | SS14e |
| **PCI-DSSV3.2.1** | 8.1.8 |
| **PCI-DSSV4.0** | 8.2.8 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 13.2 |
| **QCSC-V1** | 15.2 |
| **TBA-FIISB** | 36.2.1 |
| **TBA-FIISB** | 37.1.4 |

## Assets

### linux_project

```
The command script with multiple lines returned :

grep: : No such file or directory
grep: : No such file or directory

FAILED

TMOUT is not configured
```

## 5.4.3.3 Ensure default user umask is configured

### Info

The user file-creation mode mask ( umask ) is used to determine the file permission for newly created directories and files. In Linux, the default permissions for any newly created directory is 0777 ( rwxrwxrwx ), and for any newly created file it is 0666 ( rw-rw-rw- ). The umask modifies the default Linux permissions by restricting (masking) these permissions. The umask is not simply subtracted, but is processed bitwise. Bits set in the umask are cleared in the resulting file mode.
umask can be set with either Octal or Symbolic values:
- Octal (Numeric) Value - Represented by either three or four digits. ie umask 0027 or umask 027 If a four digit umask is used, the first digit is ignored. The remaining three digits effect the resulting permissions for user, group, and world/other respectively.
- Symbolic Value - Represented by a comma separated list for User u group g and world/other o The permissions listed are not masked by umask ie a umask set by umask u=rwx,g=rx,o= is the Symbolic equivalent of the Octal umask 027 This umask would set a newly created directory with file mode drwxr-x--- and a newly created file with file mode rw-r-----
The default umask can be set to use the pam_umask module or in a System Wide Shell Configuration File The user creating the directories or files has the discretion of changing the permissions via the chmod command, or choosing a different default umask by adding the umask command into a User Shell Configuration File (bash_profile orbashrc ), in their home directory.
Setting the default umask:
- pam_umask module:
- will set the umask according to the system default in /etc/login.defs and user settings, solving the problem of different umask settings with different shells, display managers, remote sessions etc.
- umask=<mask> value in the /etc/login.defs file is interpreted as Octal
- Setting USERGROUPS_ENAB to yes in /etc/login.defs (default):
- will enable setting of the umask group bits to be the same as owner bits. (examples: 022 -> 002, 077 -> 007) for non-root users, if the uid is the same as gid and username is the same as the <primary group name>
- userdel will remove the user's group if it contains no more members, and useradd will create by default a group with the name of the user
- System Wide Shell Configuration File :
- /etc/profile - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in thebash_profile however this file is used to set an initial PATH or PS1 for all shell users of the system. is only executed for interactive
login
shells, or shells executed with the --login parameter.
- /etc/profile.d - /etc/profile will execute the scripts within /etc/profile.d/*.sh It is recommended to place your configuration in a shell script within /etc/profile.d to set your own system wide environmental variables.
- /etc/bashrc - System wide version ofbashrc In Fedora derived distributions, etc/bashrc also invokes /etc/profile.d/*.sh if
non-login
shell, but redirects output to /dev/null if
non-interactive.
Is only executed for
interactive
shells or if BASH_ENV is set to /etc/bashrc
User Shell Configuration Files:
- ~/.bash_profile - Is executed to configure your shell before the initial command prompt. Is only read by login shells.
- ~/.bashrc - Is executed for interactive shells. only read by a shell that's both interactive and non-login
umask is set by order of precedence. If umask is set in multiple locations, this order of precedence will determine the system's default umask
Order of precedence:
- A file in /etc/profile.d/ ending insh - This will override any other system-wide umask setting
- In the file /etc/profile
- On the pam_umask.so module in /etc/pam.d/postlogin
- In the file /etc/login.defs
- In the file /etc/default/login
Setting a secure default value for umask ensures that users make a conscious choice about their file permissions. A permissive umask value could result in directories or files with excessive permissions that can be read and/or written to by unauthorized users.

### Solution

Run the following script and perform the instructions in the output to set the default umask to 027 or more restrictive:
```
#!/usr/bin/env bash
{ l_output="" l_output2="" l_out=""
file_umask_chk() { if grep -Psiq -- '^h*umaskh+(0?[0-7][2-7]7|u(=[rwx]{0,3}),g=([rx]{0,2}),o=)(h*#.*)?$' "$l_file"; then
l_out="$l_out
- umask is set correctly in \"$l_file\""
elif grep -Psiq -- '^h*umaskh+(([0-7][0-7][01][0-7]b|[0-7][0-7][0-7][0-6]b)|([0-7][01][0-7]b|[0-7][0-7][0-6]b)|(u=[rwx]{1,3},)?
(((g=[rx]?[rx]?w[rx]?[rx]?b)(,o=[rwx]{1,3})?)|((g=[wrx]{1,3},)?o=[wrx]{1,3}b)))' "$l_file"; then l_output2="$l_output2
- \"$l_file\""
fi } while IFS= read -r -d $'0' l_file; do file_umask_chk done < <(find /etc/profile.d/ -type f -name '*.sh' -print0) [ -n
"$l_out" ] && l_output="$l_out"
l_file="/etc/profile" && file_umask_chk l_file="/etc/bashrc" && file_umask_chk l_file="/etc/bash.bashrc" &&
file_umask_chk l_file="/etc/pam.d/postlogin"
if grep -Psiq '^h*sessionh+[^# r]+h+pam_umask.soh+([^# r]+h+)?umask=(([0-7][0-7][01][0-7]b|[0-7][0-7][0-7][0-6]b)|
([0-7][01][0-7]b))' "$l_file"; then l_output2="$l_output2
- \"$l_file\""
fi l_file="/etc/login.defs" && file_umask_chk l_file="/etc/default/login" && file_umask_chk if [ -z "$l_output2" ]; then
echo -e " - No files contain a UMASK that is not restrictive enough No UMASK updates required to existing files"
else echo -e "
- UMASK is not restrictive enough in the following file(s):$l_output2
- Remediation Procedure:
- Update these files and comment out the UMASK line or update umask to be \"0027\" or more restrictive"
fi if [ -n "$l_output" ]; then echo -e "$l_output"
else echo -e " - Configure UMASK in a file in the \"/etc/profile.d/\" directory ending in \".sh\"
Example Command (Hash to represent being run at a root prompt):
# printf '%s\ ' \"umask 027\" > /etc/profile.d/50-systemwide_umask.sh "
fi }
```

Notes:

- This method only applies to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked
- If the pam_umask.so module is going to be used to set umask ensure that it's not being overridden by another setting. Refer to the PAM_UMASK(8) man page for more information

## See Also

https://workbench.cisecurity.org/benchmarks/18959

## References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |

| | |
|---|---|
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |

| | |
|---|---|
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |

|  |  |
|---|---|
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - * Reasons for audit failure * :

 - umask is incorrectly set in "/etc/login.defs"
```

## 6.1.1.3 Ensure journald log file rotation is configured

### Info

Journald includes the capability of rotating log files regularly to avoid filling up the system with logs or making the logs unmanageably large. The file /etc/systemd/journald.conf is the configuration file used to specify how logs generated by Journald should be rotated.
By keeping the log files smaller and more manageable, a system administrator can easily archive these files to another system and spend less time looking through inordinately large log files.

### Solution

Edit /etc/systemd/journald.conf or a file ending inconf the /etc/systemd/journald.conf.d/ directory. Set the following parameters in the [Journal] section to ensure logs are rotated according to site policy. The settings should be carefully understood as there are specific edge cases and prioritization of parameters.
Example Configuration
:
[Journal] SystemMaxUse=1G SystemKeepFree=500M RuntimeMaxUse=200M RuntimeKeepFree=50M MaxFileSec=1month
Example script to create systemd drop-in configuration file:
{ a_settings=("SystemMaxUse=1G" "SystemKeepFree=500M" "RuntimeMaxUse=200M" "RuntimeKeepFree=50M" "MaxFileSec=1month") [ ! -d /etc/systemd/journald.conf.d/ ] && mkdir /etc/systemd/journald.conf.d/ if grep -Psq -- '^h*[Journal]' /etc/systemd/journald.conf.d/60-journald.conf; then printf '%s ' "" "${a_settings[@]}" >> /etc/systemd/journald.conf.d/60-journald.conf else printf '%s ' "" "[Journal]" "${a_settings[@]}" >> /etc/systemd/journald.conf.d/60-journald.conf fi }
Note:
- If these settings appear in a canonically later file, or later in the same file, the setting will be overwritten
- Logfile size and configuration to move logfiles to a remote log server should be accounted for when configuring these settings
Run to following command to update the parameters in the service:
# systemctl reload-or-restart systemd-journald

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171** | 3.3.6 |
| **800-171R3** | 03.03.01 |
| **800-171R3** | 03.03.03 |
| **800-171R3** | 03.03.06a. |
| **800-53** | AU-2 |
| **800-53** | AU-7 |
| **800-53** | AU-12 |
| **800-53R5** | AU-2 |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-12 |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 8.1.4.3(a) |
| **CSCV7** | 6.2 |

| | |
|---|---|
| **CSCV7** | 6.3 |
| **CSCV8** | 8.2 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | DE.CM-7 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.8.15 |
| **ITSG-33** | AU-2 |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-12 |
| **LEVEL** | 1M |
| **NESA** | M1.2.2 |
| **NESA** | M5.5.1 |
| **NIAV2** | AM7 |
| **NIAV2** | AM11a |
| **NIAV2** | AM11b |
| **NIAV2** | AM11c |
| **NIAV2** | AM11d |
| **NIAV2** | AM11e |
| **NIAV2** | SS30 |

|  |  |
|---|---|
| **NIAV2** | VL8 |
| **PCI-DSSV3.2.1** | 10.1 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:
  - Parameter: "SystemMaxUse" is not set in an included file
   *** Note: ***
   "SystemMaxUse" May be set in a file that's ignored by load procedure
  - Parameter: "SystemKeepFree" is not set in an included file
   *** Note: ***
   "SystemKeepFree" May be set in a file that's ignored by load procedure
  - Parameter: "RuntimeMaxUse" is not set in an included file
   *** Note: ***
   "RuntimeMaxUse" May be set in a file that's ignored by load procedure
  - Parameter: "RuntimeKeepFree" is not set in an included file
   *** Note: ***
   "RuntimeKeepFree" May be set in a file that's ignored by load procedure
  - Parameter: "MaxFileSec" is not set in an included file
   *** Note: ***
   "MaxFileSec" May be set in a file that's ignored by load procedure
```

## 6.1.2.1.1 Ensure systemd-journal-remote is installed

### Info

Journald systemd-journal-remote supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralized log management.
Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.
Note: This recommendation only applies if journald is the chosen method for client side logging Do not apply this recommendation if rsyslog is used.

### Solution

Run the following command to install systemd-journal-remote :
# apt install systemd-journal-remote

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171** | 3.3.6 |
| **800-171R3** | 03.03.01 |
| **800-171R3** | 03.03.03 |
| **800-171R3** | 03.03.06a. |
| **800-53** | AU-2 |
| **800-53** | AU-7 |
| **800-53** | AU-12 |
| **800-53R5** | AU-2 |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-12 |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 8.1.4.3(a) |
| **CSCV7** | 6.2 |
| **CSCV7** | 6.3 |
| **CSCV8** | 8.2 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | DE.CM-7 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |

| | |
|---|---|
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.8.15 |
| **ITSG-33** | AU-2 |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-12 |
| **LEVEL** | 1A |
| **NESA** | M1.2.2 |
| **NESA** | M5.5.1 |
| **NIAV2** | AM7 |
| **NIAV2** | AM11a |
| **NIAV2** | AM11b |
| **NIAV2** | AM11c |
| **NIAV2** | AM11d |
| **NIAV2** | AM11e |
| **NIAV2** | SS30 |
| **NIAV2** | VL8 |
| **PCI-DSSV3.2.1** | 10.1 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |

| | |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |

## Assets

### linux_project

```
The command '/bin/dpkg -s systemd-journal-remote 2>&1 | /bin/grep -E '(Status:|not installed)''
 returned :

dpkg-query: package 'systemd-journal-remote' is not installed and no information is available
```

## 6.1.2.1.2 Ensure systemd-journal-upload authentication is configured

### Info

Journald systemd-journal-upload supports the ability to send log events it gathers to a remote log host.
Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.
Note: This recommendation only applies if journald is the chosen method for client side logging Do not apply this recommendation if rsyslog is used.

### Solution

Edit the /etc/systemd/journal-upload.conf file or a file in /etc/systemd/journal-upload.conf.d ending inconf and ensure the following lines are set in the [Upload] section per your environment:
Example settings:

```
[Upload] URL=192.168.50.42 ServerKeyFile=/etc/ssl/private/journal-upload.pem ServerCertificateFile=/etc/ssl/certs/journal-upload.pem TrustedCertificateFile=/etc/ssl/ca/trusted.pem
```

Example script to create systemd drop-in configuration file:

```
#!/usr/bin/env bash
{ a_settings=("URL=192.168.50.42" "ServerKeyFile=/etc/ssl/private/journal-upload.pem" "ServerCertificateFile=/etc/ssl/certs/journal-upload.pem" "TrustedCertificateFile=/etc/ssl/ca/trusted.pem") [ ! -d /etc/systemd/journal-upload.conf.d/ ] && mkdir /etc/systemd/journal-upload.conf.d/ if grep -Psq -- '^h*[Upload]' /etc/systemd/journal-upload.conf.d/60-journald_upload.conf; then printf '%s ' "" "${a_settings[@]}" >> /etc/systemd/journal-upload.conf.d/60-journald_upload.conf else printf '%s ' "" "[Journal]" "${a_settings[@]}" >> /etc/systemd/journal-upload.conf.d/60-journald_upload.conf fi }
```

Run the following command to update the parameters in the service:

```
# systemctl reload-or-restart systemd-journal-upload
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171** | 3.3.6 |
| **800-171R3** | 03.03.01 |
| **800-171R3** | 03.03.03 |
| **800-171R3** | 03.03.06a. |
| **800-53** | AU-2 |
| **800-53** | AU-7 |
| **800-53** | AU-12 |
| **800-53R5** | AU-2 |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-12 |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 8.1.4.3(a) |
| **CSCV7** | 6.2 |
| **CSCV7** | 6.3 |
| **CSCV8** | 8.2 |

| | |
|---|---|
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | DE.CM-7 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.8.15 |
| **ITSG-33** | AU-2 |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-12 |
| **LEVEL** | 1M |
| **NESA** | M1.2.2 |
| **NESA** | M5.5.1 |
| **NIAV2** | AM7 |
| **NIAV2** | AM11a |
| **NIAV2** | AM11b |
| **NIAV2** | AM11c |
| **NIAV2** | AM11d |
| **NIAV2** | AM11e |
| **NIAV2** | SS30 |
| **NIAV2** | VL8 |
| **PCI-DSSV3.2.1** | 10.1 |

| | |
|---|---|
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:
  - Parameter: "URL" is not set in an included file
   *** Note: ***
   "URL" May be set in a file that's ignored by load procedure
  - Parameter: "ServerKeyFile" is not set in an included file
   *** Note: ***
   "ServerKeyFile" May be set in a file that's ignored by load procedure
  - Parameter: "ServerCertificateFile" is not set in an included file
   *** Note: ***
   "ServerCertificateFile" May be set in a file that's ignored by load procedure
  - Parameter: "TrustedCertificateFile" is not set in an included file
   *** Note: ***
   "TrustedCertificateFile" May be set in a file that's ignored by load procedure
```

## 6.1.2.1.3 Ensure systemd-journal-upload is enabled and active

### Info

Journald systemd-journal-upload supports the ability to send log events it gathers to a remote log host.
Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.
Note: This recommendation only applies if journald is the chosen method for client side logging Do not apply this recommendation if rsyslog is used.

### Solution

Run the following commands to unmask, enable and start systemd-journal-upload :
# systemctl unmask systemd-journal-upload.service # systemctl --now enable systemd-journal-upload.service

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171** | 3.3.6 |
| **800-171R3** | 03.03.01 |
| **800-171R3** | 03.03.03 |
| **800-171R3** | 03.03.06a. |
| **800-53** | AU-2 |
| **800-53** | AU-7 |
| **800-53** | AU-12 |
| **800-53R5** | AU-2 |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-12 |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 8.1.4.3(a) |
| **CSCV7** | 6.2 |
| **CSCV7** | 6.3 |
| **CSCV8** | 8.2 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | DE.CM-7 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | DE.CM-01 |

| | |
|---|---|
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.8.15 |
| **ITSG-33** | AU-2 |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-12 |
| **LEVEL** | 1A |
| **NESA** | M1.2.2 |
| **NESA** | M5.5.1 |
| **NIAV2** | AM7 |
| **NIAV2** | AM11a |
| **NIAV2** | AM11b |
| **NIAV2** | AM11c |
| **NIAV2** | AM11d |
| **NIAV2** | AM11e |
| **NIAV2** | SS30 |
| **NIAV2** | VL8 |
| **PCI-DSSV3.2.1** | 10.1 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |

| | |
|---|---|
| **SWIFT-CSCV1** | 6.4 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - journald enabled
The command '/bin/systemctl is-enabled systemd-journal-upload.service' returned :

not-found

-------------------------
FAILED - journald active
The command '/bin/systemctl is-active systemd-journal-upload.service' returned :

inactive
```

## 6.1.2.2 Ensure journald ForwardToSyslog is disabled

### Info

Data from journald should be kept in the confines of the service and not forwarded to other services.
- IF - journald is the method for capturing logs, all logs of the system should be handled by journald and not forwarded to other logging mechanisms.
Note: This recommendation only applies if journald is the chosen method for client side logging Do not apply this recommendation if rsyslog is used.

### Solution

- IF - rsyslog is the preferred method for capturing logs, this section and Recommendation should be skipped and the "Configure rsyslog" section followed.
- IF - journald is the preferred method for capturing logs:
Set the following parameter in the [Journal] section in /etc/systemd/journald.conf or a file in /etc/systemd/journald.conf.d/ ending inconf :
ForwardToSyslog=no
Example script to create systemd drop-in configuration file:

```
#!/usr/bin/env bash
{ a_settings=("ForwardToSyslog=no") [ ! -d /etc/systemd/journald.conf.d/ ] && mkdir /etc/systemd/journald.conf.d/
if grep -Psq -- '^h*[Journal]' /etc/systemd/journald.conf.d/60-journald.conf; then printf '%s ' "" "${a_settings[@]}"
>> /etc/systemd/journald.conf.d/60-journald.conf else printf '%s ' "" "[Journal]" "${a_settings[@]}" >> /etc/systemd/
journald.conf.d/60-journald.conf fi }
```

Note: If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten
Run to following command to update the parameters in the service:

```
# systemctl reload-or-restart systemd-journald
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171** | 3.3.6 |
| **800-171R3** | 03.03.01 |
| **800-171R3** | 03.03.03 |
| **800-171R3** | 03.03.06a. |
| **800-53** | AU-2 |
| **800-53** | AU-7 |
| **800-53** | AU-12 |
| **800-53R5** | AU-2 |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-12 |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 8.1.4.3(a) |
| **CSCV7** | 6.3 |
| **CSCV8** | 8.2 |
| **CSF** | DE.CM-1 |

| | |
|---|---|
| **CSF** | DE.CM-3 |
| **CSF** | DE.CM-7 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.8.15 |
| **ITSG-33** | AU-2 |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-12 |
| **LEVEL** | 1A |
| **NESA** | M1.2.2 |
| **NESA** | M5.5.1 |
| **NIAV2** | AM7 |
| **NIAV2** | AM11a |
| **NIAV2** | AM11b |
| **NIAV2** | AM11c |
| **NIAV2** | AM11d |
| **NIAV2** | AM11e |
| **NIAV2** | SS30 |
| **NIAV2** | VL8 |
| **PCI-DSSV3.2.1** | 10.1 |
| **QCSC-V1** | 3.2 |

|  |  |
|---|---|
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:
  - Parameter: "ForwardToSyslog"
    incorrectly set to: "yes"
    in the file: "/usr/lib/systemd/journald.conf.d/syslog.conf"
    Should be set to: "no"
```

## 6.1.2.3 Ensure journald Compress is configured

### Info

The journald system includes the capability of compressing overly large files to avoid filling up the system with logs or making the logs unmanageably large.
Uncompressed large files may unexpectedly fill a filesystem leading to resource unavailability. Compressing logs prior to write can prevent sudden, unexpected filesystem impacts.
Note: This recommendation only applies if journald is the chosen method for client side logging Do not apply this recommendation if rsyslog is used.

### Solution

- IF - rsyslog is the preferred method for capturing logs, this section and Recommendation should be skipped and the "Configure rsyslog" section followed.
- IF - journald is the preferred method for capturing logs:
Set the following parameter in the [Journal] section in /etc/systemd/journald.conf or a file in /etc/systemd/journald.conf.d/ ending inconf :
Compress=yes
Example script to create systemd drop-in configuration file:
#!/usr/bin/env bash
{ a_settings=("Compress=yes") [ ! -d /etc/systemd/journald.conf.d/ ] && mkdir /etc/systemd/journald.conf.d/ if grep -Psq -- '^h*[Journal]' /etc/systemd/journald.conf.d/60-journald.conf; then printf '%s ' "" "${a_settings[@]}" >> /etc/systemd/journald.conf.d/60-journald.conf else printf '%s ' "" "[Journal]" "${a_settings[@]}" >> /etc/systemd/journald.conf.d/60-journald.conf fi }
Note: If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten
Run to following command to update the parameters in the service:
# systemctl reload-or-restart systemd-journald

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171** | 3.3.6 |
| **800-171R3** | 03.03.01 |
| **800-171R3** | 03.03.03 |
| **800-171R3** | 03.03.06a. |
| **800-53** | AU-2 |
| **800-53** | AU-4 |
| **800-53** | AU-7 |
| **800-53** | AU-12 |
| **800-53R5** | AU-2 |
| **800-53R5** | AU-4 |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-12 |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 8.1.4.3(a) |

| | |
|---|---|
| **CSCV7** | 6.2 |
| **CSCV7** | 6.3 |
| **CSCV7** | 6.4 |
| **CSCV8** | 8.2 |
| **CSCV8** | 8.3 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | DE.CM-7 |
| **CSF** | PR.DS-4 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.8.6 |
| **ISO-27001-2022** | A.8.15 |
| **ITSG-33** | AU-2 |
| **ITSG-33** | AU-4 |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-12 |
| **LEVEL** | 1A |
| **NESA** | M1.2.2 |
| **NESA** | M5.5.1 |
| **NESA** | T3.3.1 |

|  |  |
|---|---|
| **NESA** | T3.6.2 |
| **NIAV2** | AM7 |
| **NIAV2** | AM11a |
| **NIAV2** | AM11b |
| **NIAV2** | AM11c |
| **NIAV2** | AM11d |
| **NIAV2** | AM11e |
| **NIAV2** | SS30 |
| **NIAV2** | VL8 |
| **PCI-DSSV3.2.1** | 10.1 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:
  - Parameter: "Compress" is not set in an included file
   *** Note: "Compress" May be set in a file that's ignored by load procedure ***
```

## 6.1.2.4 Ensure journald Storage is configured

### Info

Data from journald may be stored in volatile memory or persisted locally on the server. Logs in memory will be lost upon a system reboot. By persisting logs to local disk on the server they are protected from loss due to a reboot. Writing log data to disk will provide the ability to forensically reconstruct events which may have impacted the operations or security of a system even after a system crash or reboot.
Note: This recommendation only applies if journald is the chosen method for client side logging Do not apply this recommendation if rsyslog is used.

### Solution

- IF - rsyslog is the preferred method for capturing logs, this section and Recommendation should be skipped and the "Configure rsyslog" section followed.
- IF - journald is the preferred method for capturing logs:
Set the following parameter in the [Journal] section in /etc/systemd/journald.conf or a file in /etc/systemd/journald.conf.d/ ending inconf :

```
Storage=persistent
```

Example script to create systemd drop-in configuration file:

```
#!/usr/bin/env bash
{ a_settings=("Storage=persistent") [ ! -d /etc/systemd/journald.conf.d/ ] && mkdir /etc/systemd/journald.conf.d/
if grep -Psq -- '^h*[Journal]' /etc/systemd/journald.conf.d/60-journald.conf; then printf '%s ' "" "${a_settings[@]}"
>> /etc/systemd/journald.conf.d/60-journald.conf else printf '%s ' "" "[Journal]" "${a_settings[@]}" >> /etc/systemd/journald.conf.d/60-journald.conf fi }
```

Note: If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten
Run to following command to update the parameters in the service:

```
# systemctl reload-or-restart systemd-journald
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171** | 3.3.6 |
| **800-171R3** | 03.03.01 |
| **800-171R3** | 03.03.03 |
| **800-171R3** | 03.03.06a. |
| **800-53** | AU-2 |
| **800-53** | AU-7 |
| **800-53** | AU-12 |
| **800-53R5** | AU-2 |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-12 |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 8.1.4.3(a) |
| **CSCV7** | 6.2 |
| **CSCV7** | 6.3 |

| | |
|---|---|
| **CSCV8** | 8.2 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | DE.CM-7 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.8.15 |
| **ITSG-33** | AU-2 |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-12 |
| **LEVEL** | 1A |
| **NESA** | M1.2.2 |
| **NESA** | M5.5.1 |
| **NIAV2** | AM7 |
| **NIAV2** | AM11a |
| **NIAV2** | AM11b |
| **NIAV2** | AM11c |
| **NIAV2** | AM11d |
| **NIAV2** | AM11e |
| **NIAV2** | SS30 |
| **NIAV2** | VL8 |

| | |
|---|---|
| **PCI-DSSV3.2.1** | 10.1 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:
  - Parameter: "Storage" is not set in an included file
   *** Note: "Storage" May be set in a file that's ignored by load procedure ***
```

## 6.1.3.6 Ensure rsyslog is configured to send logs to a remote log host

### Info

rsyslog supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralized log management.

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

### Solution

Edit the rsyslog configuration and add the following line (where loghost.example.com is the name of your central log host). The target directive may either be a fully qualified domain name or an IP address.

Example script to create a drop-in configuration file:

```
#!/usr/bin/env bash
{ a_parameters=('*.* action(type="omfwd" target="loghost.example.com" port="514" protocol="tcp"' '
action.resumeRetryCount="100"' ' queue.type="LinkedList" queue.size="1000")') [ ! -d "/etc/rsyslog.d/" ] && mkdir /etc/
rsyslod.d/ printf '%s ' "" "${a_parameters[@]}" >> /etc/rsyslog.d/60-rsyslog.conf }
```

Run the following command to reload rsyslog.service :

```
# systemctl reload-or-restart rsyslog.service
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171** | 3.3.6 |
| **800-171R3** | 03.03.01 |
| **800-171R3** | 03.03.03 |
| **800-171R3** | 03.03.06a. |
| **800-53** | AU-2 |
| **800-53** | AU-7 |
| **800-53** | AU-12 |
| **800-53R5** | AU-2 |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-12 |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 8.1.4.3(a) |
| **CSCV7** | 6.2 |
| **CSCV7** | 6.3 |
| **CSCV8** | 8.2 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | DE.CM-7 |

| | |
|---|---|
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.8.15 |
| **ITSG-33** | AU-2 |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-12 |
| **LEVEL** | 1M |
| **NESA** | M1.2.2 |
| **NESA** | M5.5.1 |
| **NIAV2** | AM7 |
| **NIAV2** | AM11a |
| **NIAV2** | AM11b |
| **NIAV2** | AM11c |
| **NIAV2** | AM11d |
| **NIAV2** | AM11e |
| **NIAV2** | SS30 |
| **NIAV2** | VL8 |
| **PCI-DSSV3.2.1** | 10.1 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |

|  |  |
|---|---|
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |

## Assets

### linux_project

```
One of the following must pass to satisfy this requirement:

-------------------------
FAILED - Ensure logs are sent to a central host - basic format
The command script with multiple lines did not return any result

-------------------------
FAILED - Ensure logs are sent to a central host - advanced format
The command script with multiple lines did not return any result
```

## 6.1.4.1 Ensure access to all logfiles has been configured

### Info

Log files contain information from many services on the the local system, or in the event of a centralized log server, others systems logs as well.
In general log files are found in /var/log/ although application can be configured to store logs elsewhere. Should your application store logs in another, ensure to run the same test on that location.
It is important that log files have the correct permissions to ensure that sensitive data is protected and that only the appropriate users / groups have access to them.

### Solution

Run the following script to update permissions and ownership on files in /var/log
Although the script is not destructive, ensure that the output of the audit procedure is captured in the event that the remediation causes issues.

```
#!/usr/bin/env bash
{ a_output2=() f_file_test_fix() { a_out2=() maxperm="$( printf '%o' $(( 0777 & ~$perm_mask)) )"
if [ $(( $l_mode & $perm_mask )) -gt 0 ]; then a_out2+=(" o Mode: \"$l_mode\" should be \"$maxperm\" or more
restrictive" " x Removing excess permissions") chmod "$l_rperms" "$l_fname"
fi if [[ ! "$l_user" =~ $l_auser ]]; then a_out2+=(" o Owned by: \"$l_user\" and should be owned by \"${l_auser//|/ or }\""
" x Changing ownership to: \"$l_fix_account\"") chown "$l_fix_account" "$l_fname"
fi if [[ ! "$l_group" =~ $l_agroup ]]; then a_out2+=(" o Group owned by: \"$l_group\" and should be group owned by
\"${l_agroup//|/ or }\"" " x Changing group ownership to: \"$l_fix_account\"") chgrp "$l_fix_account" "$l_fname"
fi [ "${#a_out2[@]}" -gt 0 ] && a_output2+=(" - File: \"$l_fname\" is:" "${a_out2[@]}") } l_fix_account='root'
while IFS= read -r -d $'0' l_file; do while IFS=: read -r l_fname l_mode l_user l_group; do if grep -Pq -- '/(apt)h*$'
<<< "$(dirname "$l_fname")"; then perm_mask='0133' l_rperms="u-x,go-wx" l_auser="root" l_agroup="(root|adm)";
f_file_test_fix else case "$(basename "$l_fname")" in lastlog | lastlog.* | wtmp | wtmp.* | wtmp-* | btmp | btmp.* | btmp-
* | README) perm_mask='0113' l_rperms="ug-x,o-wx" l_auser="root" l_agroup="(root|utmp)"
f_file_test_fix ;;
cloud-init.log* | localmessages* | waagent.log*) perm_mask='0133' l_rperms="u-x,go-wx" l_auser="(root|syslog)"
l_agroup="(root|adm)"
f_file_test_fix ;;
secure | auth.log | syslog | messages) perm_mask='0137' l_rperms="u-x,g-wx,o-rwx" l_auser="(root|syslog)"
l_agroup="(root|adm)"
f_file_test_fix ;;
SSSD | sssd) perm_mask='0117' l_rperms="ug-x,o-rwx" l_auser="(root|SSSD)" l_agroup="(root|SSSD)"
f_file_test_fix ;;
gdm | gdm3) perm_mask='0117' l_rperms="ug-x,o-rwx" l_auser="root" l_agroup="(root|gdm|gdm3)"
f_file_test_fix ;;
*.journal | *.journal~) perm_mask='0137' l_rperms="u-x,g-wx,o-rwx" l_auser="root" l_agroup="(root|systemd-journal)"
f_file_test_fix ;;
*) perm_mask='0137' l_rperms="u-x,g-wx,o-rwx" l_auser="(root|syslog)" l_agroup="(root|adm)"
if [ "$l_user" = "root" ] || ! grep -Pq -- "^h*$(awk -F: '$1==""$l_user"" {print $7}' /etc/passwd)b" /etc/shells; then ! grep -
Pq -- "$l_auser" <<< "$l_user" && l_auser="(root|syslog|$l_user)"
! grep -Pq -- "$l_agroup" <<< "$l_group" && l_agroup="(root|adm|$l_group)"
fi f_file_test_fix ;;
esac fi done < <(stat -Lc '%n:%#a:%U:%G' "$l_file") done < <(find -L /var/log -type f ( -perm /0137 -o ! -user root -o ! -
group root ) -print0) if [ "${#a_output2[@]}" -le 0 ]; then # If all files passed, then we report no changes a_output+=(" -
All files in \"/var/log/\" have appropriate permissions and ownership") printf '
%s' "- All files in \"/var/log/\" have appropriate permissions and ownership" " o No changes required" ""
else printf '
%s' "${a_output2[@]}" ""
fi }
```

Note: You may also need to change the configuration for your logging software or services for any logs that had incorrect permissions.
If there are services that log to other locations, ensure that those log files have the appropriate permissions.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |

| | |
|---|---|
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |

| | |
|---|---|
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |

| | |
|---|---|
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
 The command script with multiple lines returned :

/bin/bash: line 28: file_test_chk: command not found

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:
 - File: "/var/log/alternatives.log.1" is:
   o Mode: "0644" should be "640" or more restrictive
 - File: "/var/log/dpkg.log.1" is:
   o Mode: "0644" should be "640" or more restrictive
 - File: "/var/log/sysstat/sa30" is:
   o Mode: "0644" should be "640" or more restrictive
 - File: "/var/log/sysstat/sar02" is:
   o Mode: "0644" should be "640" or more restrictive
 - File: "/var/log/sysstat/sa02" is:
   o Mode: "0644" should be "640" or more restrictive
 - File: "/var/log/sysstat/sa28" is:
    o Mode: "0644" should be "640" or more restrictive
  - File: "/var/log/sysstat/sa01" is:
    o Mode: "0644" should be "640" or more restrictive
  - File: "/var/log/sysstat/sar25" is:
    o Mode: "0644" should be "640" or more restrictive
  - File: "/var/log/sysstat/sar26" is:
    o Mode: "0644" should be "640" or more restrictive
  - File: "/var/log/sysstat/sar28" is:
    o Mode: "0644" should be "640" or more restrictive
  - File: "/var/log/sysstat/sa27" is:
    o Mode: "0644" should be "640" or more restrictive
  - File: "/var/log/sysstat/sar27" is:
    o Mode: "0644" should be "640" or more restrictive
  - File: "/var/log/sysstat/sa25" is:
    o Mode: "0644" should be "640" or more restrictive
  - File: "/var/log/sysstat/sar29" is:
    o Mode: "0644" should be "640" or more restrictive
  - File: "/var/log/sysstat/sa03" is:
    o Mode: "0644" should be "640" or more restrictive
  - File: "/var/log/sysstat/sa29" is:
    o [...]
```

## 6.3.1 Ensure AIDE is installed

### Info

AIDE takes a snapshot of filesystem state including modification times, permissions, and file hashes which can then be used to compare against the current state of the filesystem to detect modifications to the system.
By monitoring the filesystem state compromised files can be detected to prevent or limit the exposure of accidental or malicious misconfigurations or modified binaries.

### Solution

Install AIDE using the appropriate package manager or manual installation:
# apt install aide aide-common
Configure AIDE as appropriate for your environment. Consult the AIDE documentation for options.
Run the following commands to initialize AIDE:
# aideinit # mv /var/lib/aide/aide.db.new /var/lib/aide/aide.db

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.7 |
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171R3** | 03.01.07b. |
| **800-171R3** | 03.03.01 |
| **800-171R3** | 03.03.03 |
| **800-53** | AC-6(9) |
| **800-53** | AU-2 |
| **800-53** | AU-12 |
| **800-53R5** | AC-6(9) |
| **800-53R5** | AU-2 |
| **800-53R5** | AU-12 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.3(a) |
| **CN-L3** | 8.1.10.6(a) |
| **CSCV7** | 14.9 |
| **CSCV8** | 3.14 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | DE.CM-7 |

| | |
|---|---|
| **CSF** | PR.AC-4 |
| **CSF** | PR.PT-1 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.PS-04 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.15 |
| **ISO-27001-2022** | A.8.18 |
| **ISO/IEC-27001** | A.12.4.3 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | AU-2 |
| **ITSG-33** | AU-12 |
| **LEVEL** | 1A |
| **NESA** | M1.2.2 |
| **NESA** | M5.5.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.5.4 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM7 |
| **NIAV2** | AM11a |
| **NIAV2** | AM11b |
| **NIAV2** | AM11c |

| | |
|---|---|
| **NIAV2** | AM11d |
| **NIAV2** | AM11e |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS30 |
| **NIAV2** | VL8 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV3.2.1** | 10.1 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **SWIFT-CSCV1** | 6.4 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - dpkg check aide-common
The command '/bin/dpkg -s aide-common 2>&1 | /bin/grep -E '(Status:|not installed)'' returned :

dpkg-query: package 'aide-common' is not installed and no information is available

-------------------------
FAILED - dpkg check aide
The command '/bin/dpkg -s aide 2>&1 | /bin/grep -E '(Status:|not installed)'' returned :

dpkg-query: package 'aide' is not installed and no information is available
```

## 6.3.2 Ensure filesystem integrity is regularly checked

### Info

Periodic checking of the filesystem integrity is needed to detect changes to the filesystem.
Periodic file checking allows the system administrator to determine on a regular basis if critical files have been changed in an unauthorized fashion.

### Solution

Run the following command to unmask dailyaidecheck.timer and dailyaidecheck.service :
# systemctl unmask dailyaidecheck.timer dailyaidecheck.service
Run the following command to enable and start dailyaidecheck.timer :
# systemctl --now enable dailyaidecheck.timer

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171** | 3.3.6 |
| **800-171R3** | 03.03.02a. |
| **800-171R3** | 03.03.02b. |
| **800-171R3** | 03.03.03 |
| **800-171R3** | 03.03.06a. |
| **800-53** | AU-3 |
| **800-53** | AU-3(1) |
| **800-53** | AU-7 |
| **800-53** | AU-12 |
| **800-53R5** | AU-3 |
| **800-53R5** | AU-3(1) |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-12 |
| **CN-L3** | 7.1.2.3(a) |
| **CN-L3** | 7.1.2.3(b) |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 7.1.3.3(a) |
| **CN-L3** | 7.1.3.3(b) |
| **CN-L3** | 8.1.4.3(b) |
| **CSCV7** | 14.9 |
| **CSCV8** | 8.5 |

| | |
|---|---|
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | DE.CM-7 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.5.28 |
| **ISO-27001-2022** | A.8.15 |
| **ITSG-33** | AU-3 |
| **ITSG-33** | AU-3(1) |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-12 |
| **LEVEL** | 1A |
| **NESA** | T3.6.2 |
| **NIAV2** | AM34a |
| **NIAV2** | AM34b |
| **NIAV2** | AM34c |
| **NIAV2** | AM34d |
| **NIAV2** | AM34e |
| **NIAV2** | AM34f |
| **NIAV2** | AM34g |
| **PCI-DSSV3.2.1** | 10.1 |

| | |
|---|---|
| **PCI-DSSV3.2.1** | 10.3 |
| **PCI-DSSV3.2.1** | 10.3.1 |
| **PCI-DSSV3.2.1** | 10.3.2 |
| **PCI-DSSV3.2.1** | 10.3.3 |
| **PCI-DSSV3.2.1** | 10.3.4 |
| **PCI-DSSV3.2.1** | 10.3.5 |
| **PCI-DSSV3.2.1** | 10.3.6 |
| **PCI-DSSV4.0** | 10.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
FAILED - dailyaidecheck.timer enabled
The command '/bin/systemctl list-unit-files | /bin/awk '$1~/^dailyaidecheck\.(timer|service)$/
{print $1 "\t" $2}'' did not return any result

-------------------------
FAILED - dailyaidecheck.service static
The command '/bin/systemctl list-unit-files | /bin/awk '$1~/^dailyaidecheck\.(timer|service)$/
{print $1 "\t" $2}'' did not return any result

-------------------------
FAILED - aidecheck active
The command '/bin/systemctl is-active dailyaidecheck.timer' returned :

inactive
```

## 7.1.11 Ensure world writable files and directories are secured

### Info

World writable files are the least secure. Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity. See the chmod(2) man page for more information.
Setting the sticky bit on world writable directories prevents users from deleting or renaming files in that directory that are not owned by them.
Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.
This feature prevents the ability to delete or rename files in world writable directories (such as /tmp ) that are owned by another user.

### Solution

- World Writable Files:
- It is recommended that write access is removed from other with the command ( chmod o-w <filename> ), but always consult relevant vendor documentation to avoid breaking any application dependencies on a given file.
- World Writable Directories:
- Set the sticky bit on all world writable directories with the command ( chmod a+t <directory_name> )
Run the following script to:
- Remove other write permission from any world writable files
- Add the sticky bit to all world writable directories

```
#!/usr/bin/env bash
{ l_smask='01000'
a_file=(); a_dir=() # Initialize arrays a_path=(! -path "/run/user/*" -a ! -path "/proc/*" -a ! -path "*/containerd/*" -a ! -path
"*/kubelet/pods/*" -a ! -path "*/kubelet/plugins/*" -a ! -path "/sys/*" -a ! -path "/snap/*") while IFS= read -r l_mount; do
while IFS= read -r -d $'0' l_file; do if [ -e "$l_file" ]; then l_mode="$(stat -Lc '%#a' "$l_file")"
if [ -f "$l_file" ]; then # Remove excess permissions from WW files echo -e " - File: \"$l_file\" is mode: \"$l_mode\"
- removing write permission on \"$l_file\" from \"other\""
chmod o-w "$l_file"
fi if [ -d "$l_file" ]; then # Add sticky bit if [ ! $(( $l_mode & $l_smask )) -gt 0 ]; then echo -e " - Directory: \"$l_file\" is
mode: \"$l_mode\" and doesn't have the sticky bit set
- Adding the sticky bit"
chmod a+t "$l_file"
fi fi fi done < <(find "$l_mount" -xdev ( "${a_path[@]}" ) ( -type f -o -type d ) -perm -0002 -print0 2> /dev/null) done <
<(findmnt -Dkerno fstype,target | awk '($1 !~ /^s*(nfs|proc|smb|vfat|iso9660|efivarfs|selinuxfs)/ && $2 !~ /^(/run/user/|/
tmp|/var/tmp)/){print $2}') }
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |

| | |
|---|---|
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |

| | |
|---|---|
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |

|  |  |
|---|---|
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The following 1 files are world writeable:

  /etc/monarx-agent.conf
     owner: root, group: root, permissions: 0666
```

## 7.1.12 Ensure no files or directories without an owner and a group exist

### Info

Administrators may delete users or groups from the system and neglect to remove all files and/or directories owned by those users or groups.
A new user or group who is assigned a deleted user's user ID or group ID may then end up "owning" a deleted user or group's files, and thus have more access on the system than was intended.

### Solution

Remove or set ownership and group ownership of these files and/or directories to an active user on the system as appropriate.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |

| | |
|---|---|
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |

| | |
|---|---|
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |

| | |
|---|---|
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
 The command script with multiple lines returned :

- Audit Result:
  ** FAIL **
 - * Reasons for audit failure * :

  - There are "11" unowned files or directories on the system.
   - The following is a list of unowned files and/or directories:
/ruta/a/tu/config/etc/licenses
/ruta/a/tu/config/etc/tmp/web
/var/lib/docker/overlay2/608a8667012c41228a1913b77395d8f57bebf7651c767e6166b699579dca4f3f/diff/
usr/local/bin/railpack
/var/lib/docker/overlay2/608a8667012c41228a1913b77395d8f57bebf7651c767e6166b699579dca4f3f/diff/
usr/local/bin/README.md
/var/lib/docker/overlay2/608a8667012c41228a1913b77395d8f57bebf7651c767e6166b699579dca4f3f/diff/
usr/local/bin/LICENSE
/var/lib/docker/overlay2/71109963d19f5a6f129842ba81e6cfbe90cfbd5dd66a43462b7f6463f9a8fb50/diff/
usr/local/bin/nixpacks
/var/lib/docker/overlay2/f1359c477a6a9b0390f7298450e34318ba81afe5f8affe10f3c8789b78a5c005/diff/
app/node_modules/.pnpm/sqlite3@5.1.7/node_modules/sqlite3/build
/var/lib/docker/overlay2/f1359c477a6a9b0390f7298450e34318ba81afe5f8affe10f3c8789b78a5c005/diff/
app/node_modules/.pnpm/sqlite3@5.1.7/node_modules/sqlite3/build/Release
/var/lib/docker/overlay2/f1359c477a6a9b0390f7298450e34318ba81afe5f8affe10f3c8789b78a5c005/diff/
app/node_modules/.pnpm/sqlite3@5.1.7/node_modules/sqlite3/build/Release/node_sqlite3.node
/var/lib/docker/overlay2/f1359c477a6a9b0390f7298450e34318ba81afe5f8affe10f3c8789b78a5c005/diff/
app/node_modules/.pnpm/bcrypt@5.1.1_encoding@0.1.13/node_modules/bcrypt/lib/binding/napi-v3/
bcrypt_lib.node
/var/lib/docker/overlay2/3cc572f8cda1da4f15a3f9c65550d49532234da506ac15d095d3253243882e79/diff/
usr/local/bin/traefik
   - end of list
  - There are "7" ungrouped files or directories on the system.
   - The following is a list of ungrouped files and/or [...]
```

# Audits SKIPPED

# Audits PASSED

## 1.1.1.1 Ensure cramfs kernel module is not available

### Info

The cramfs filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A cramfs image can be used without having to first decompress the image.
Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

### Solution

Run the following script to unload and disable the cramfs module:
- IF - the cramfs kernel module is available in ANY installed kernel:
- Create a file ending inconf with install cramfs /bin/false in the /etc/modprobe.d/ directory
- Create a file ending inconf with blacklist cramfs in the /etc/modprobe.d/ directory
- Run modprobe -r cramfs 2>/dev/null; rmmod cramfs 2>/dev/null to remove cramfs from the kernel
- IF - the cramfs kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

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

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |

| | |
|---|---|
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **
 - kernel module: "cramfs" doesn't exist in "/usr/lib/modules/6.8.0-57-generic/kernel/fs"
 - kernel module: "cramfs" doesn't exist in "/usr/lib/modules/6.8.0-58-generic/kernel/fs"
```

## 1.1.1.2 Ensure freevxfs kernel module is not available

### Info

The freevxfs filesystem type is a free version of the Veritas type filesystem. This is the primary filesystem type for HP-UX operating systems.
Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

### Solution

Run the following script to unload and disable the freevxfs module:
- IF - the freevxfs kernel module is available in ANY installed kernel:
- Create a file ending inconf with install freevxfs /bin/false in the /etc/modprobe.d/ directory
- Create a file ending inconf with blacklist freevxfs in the /etc/modprobe.d/ directory
- Run modprobe -r freevxfs 2>/dev/null; rmmod freevxfs 2>/dev/null to remove freevxfs from the kernel
- IF - the freevxfs kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

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

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |

|  |  |
|---|---|
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **
 - kernel module: "freevxfs" doesn't exist in "/usr/lib/modules/6.8.0-57-generic/kernel/fs"
 - kernel module: "freevxfs" doesn't exist in "/usr/lib/modules/6.8.0-58-generic/kernel/fs"
```

## 1.1.1.3 Ensure hfs kernel module is not available

### Info

The hfs filesystem type is a hierarchical filesystem that allows you to mount Mac OS filesystems.
Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

### Solution

Run the following script to unload and disable the hfs module:
- IF - the hfs kernel module is available in ANY installed kernel:
- Create a file ending inconf with install hfs /bin/false in the /etc/modprobe.d/ directory
- Create a file ending inconf with blacklist hfs in the /etc/modprobe.d/ directory
- Run modprobe -r hfs 2>/dev/null; rmmod hfs 2>/dev/null to remove hfs from the kernel
- IF - the hfs kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

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

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |

|  |  |
|---|---|
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **
 - kernel module: "hfs" doesn't exist in "/usr/lib/modules/6.8.0-57-generic/kernel/fs"
 - kernel module: "hfs" doesn't exist in "/usr/lib/modules/6.8.0-58-generic/kernel/fs"
```

## 1.1.1.4 Ensure hfsplus kernel module is not available

### Info

The hfsplus filesystem type is a hierarchical filesystem designed to replace hfs that allows you to mount Mac OS filesystems.
Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

### Solution

Run the following script to unload and disable the hfsplus module:
- IF - the hfsplus kernel module is available in ANY installed kernel:
- Create a file ending inconf with install hfsplus /bin/false in the /etc/modprobe.d/ directory
- Create a file ending inconf with blacklist hfsplus in the /etc/modprobe.d/ directory
- Run modprobe -r hfsplus 2>/dev/null; rmmod hfsplus 2>/dev/null to remove hfsplus from the kernel
- IF - the hfsplus kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

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

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |

|  |  |
|---|---|
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **
 - kernel module: "hfsplus" doesn't exist in "/usr/lib/modules/6.8.0-57-generic/kernel/fs"
 - kernel module: "hfsplus" doesn't exist in "/usr/lib/modules/6.8.0-58-generic/kernel/fs"
```

## 1.1.1.5 Ensure jffs2 kernel module is not available

### Info

The jffs2 (journaling flash filesystem 2) filesystem type is a log-structured filesystem used in flash memory devices. Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

### Solution

Run the following script to unload and disable the jffs2 module:
- IF - the jffs2 kernel module is available in ANY installed kernel:
- Create a file ending inconf with install jffs2 /bin/false in the /etc/modprobe.d/ directory
- Create a file ending inconf with blacklist jffs2 in the /etc/modprobe.d/ directory
- Run modprobe -r jffs2 2>/dev/null; rmmod jffs2 2>/dev/null to remove jffs2 from the kernel
- IF - the jffs2 kernel module is not available on the system, or pre-compiled into the kernel, no remediation is necessary

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

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |

| | |
|---|---|
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **
 - kernel module: "jffs2" doesn't exist in "/usr/lib/modules/6.8.0-57-generic/kernel/fs"
 - kernel module: "jffs2" doesn't exist in "/usr/lib/modules/6.8.0-58-generic/kernel/fs"
```

## 1.1.2.1.2 Ensure nodev option set on /tmp partition

### Info

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

### Solution

- IF - a separate partition exists for /tmp
Edit the /etc/fstab file and add nodev to the fourth field (mounting options) for the /tmp partition.
Example:
<device> /tmp <fstype> defaults,rw,nosuid,nodev,noexec,relatime 0 0
Run the following command to remount /tmp with the configured options:
# mount -o remount /tmp

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |

|  |  |
|---|---|
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
No matching files were found
```

## 1.1.2.1.3 Ensure nosuid option set on /tmp partition

### Info

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

### Solution

- IF - a separate partition exists for /tmp
Edit the /etc/fstab file and add nosuid to the fourth field (mounting options) for the /tmp partition.
Example:
<device> /tmp <fstype> defaults,rw,nosuid,nodev,noexec,relatime 0 0
Run the following command to remount /tmp with the configured options:
# mount -o remount /tmp

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |

| | |
|---|---|
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |

| | |
|---|---|
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |

| | |
|---|---|
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
No matching files were found
```

## 1.1.2.1.4 Ensure noexec option set on /tmp partition

### Info

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

### Solution

- IF - a separate partition exists for /tmp
Edit the /etc/fstab file and add noexec to the fourth field (mounting options) for the /tmp partition.
Example:
<device> /tmp <fstype> defaults,rw,nosuid,nodev,noexec,relatime 0 0
Run the following command to remount /tmp with the configured options:
# mount -o remount /tmp
Impact:
Setting the noexec option on /tmp may prevent installation and/or updating of some 3rd party software.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |

| | |
|---|---|
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |

| | |
|---|---|
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |

| | |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
No matching files were found
```

## 1.1.2.2.1 Ensure /dev/shm is a separate partition

### Info

The /dev/shm directory is a world-writable directory that can function as shared memory that facilitates inter process communication (IPC).
Making /dev/shm its own file system allows an administrator to set additional mount options such as the noexec option on the mount, making /dev/shm useless for an attacker to install executable code. It would also prevent an attacker from establishing a hard link to a system setuid program and wait for it to be updated. Once the program was updated, the hard link would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.
This can be accomplished by mounting tmpfs to /dev/shm

### Solution

For specific configuration requirements of the /dev/shm mount for your environment, modify /etc/fstab
Example:
tmpfs /dev/shm tmpfs defaults,rw,nosuid,nodev,noexec,relatime,size=2G 0 0
Impact:
Since the /dev/shm directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition.
/dev/shm utilizing tmpfs can be resized using the size={size} parameter in the relevant entry in /etc/fstab

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |

| | |
|---|---|
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/dev/shm[\s]+' found - expect '[\s]+/dev/shm[\s]+' found
 in the following lines:
          8: 31 26 0:26 / /dev/shm rw,nosuid,nodev shared:4 - tmpfs tmpfs rw,inode64
```

## 1.1.2.2.2 Ensure nodev option set on /dev/shm partition

### Info

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

### Solution

- IF - a separate partition exists for /dev/shm
Edit the /etc/fstab file and add nodev to the fourth field (mounting options) for the /dev/shm partition. See the fstab(5) manual page for more information.
Example:

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

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

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

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

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |

| | |
|---|---|
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |

| | |
|---|---|
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |

| | |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/dev/shm[\s]+' found - expect 'nodev' found in the
 following lines:
          8: 31 26 0:26 / /dev/shm rw,nosuid,nodev shared:4 - tmpfs tmpfs rw,inode64
```

## 1.1.2.2.3 Ensure nosuid option set on /dev/shm partition

### Info

The nosuid mount option specifies that the filesystem cannot contain setuid files.
Setting this option on a file system prevents users from introducing privileged programs onto the system and allowing non-root users to execute them.

### Solution

- IF - a separate partition exists for /dev/shm
Edit the /etc/fstab file and add nosuid to the fourth field (mounting options) for the /dev/shm partition. See the fstab(5) manual page for more information.
Example:
tmpfs /dev/shm tmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0
Run the following command to remount /dev/shm with the configured options:
# mount -o remount /dev/shm
Note: It is recommended to use tmpfs as the device/filesystem type as /dev/shm is used as shared memory space by applications.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |

| | |
|---|---|
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |

| | |
|---|---|
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |

| | |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/dev/shm[\s]+' found - expect 'nosuid' found in the
 following lines:
          8: 31 26 0:26 / /dev/shm rw,nosuid,nodev shared:4 - tmpfs tmpfs rw,inode64
```

## 1.1.2.3.2 Ensure nodev option set on /home partition

### Info

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

### Solution

- IF - a separate partition exists for /home
Edit the /etc/fstab file and add nodev to the fourth field (mounting options) for the /home partition.
Example:
<device> /home <fstype> defaults,rw,nosuid,nodev,noexec,relatime 0 0
Run the following command to remount /home with the configured options:
# mount -o remount /home

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |

| | |
|---|---|
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |

| | |
|---|---|
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |

| | |
|---|---|
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
No matching files were found
```

## 1.1.2.3.3 Ensure nosuid option set on /home partition

### Info

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

### Solution

- IF - a separate partition exists for /home
Edit the /etc/fstab file and add nosuid to the fourth field (mounting options) for the /home partition.
Example:
<device> /home <fstype> defaults,rw,nosuid,nodev,noexec,relatime 0 0
Run the following command to remount /home with the configured options:
# mount -o remount /home

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |

| | |
|---|---|
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |

| | |
|---|---|
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |

| | |
|---|---|
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
No matching files were found
```

## 1.1.2.4.2 Ensure nodev option set on /var partition

### Info

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

### Solution

- IF - a separate partition exists for /var
Edit the /etc/fstab file and add nodev to the fourth field (mounting options) for the /var partition.
Example:
<device> /var <fstype> defaults,rw,nosuid,nodev,noexec,relatime 0 0
Run the following command to remount /var with the configured options:
# mount -o remount /var

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |

| | |
|---|---|
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |

| | |
|---|---|
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |

| | |
|---|---|
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
No matching files were found
```

## 1.1.2.4.3 Ensure nosuid option set on /var partition

### Info

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

### Solution

- IF - a separate partition exists for /var
Edit the /etc/fstab file and add nosuid to the fourth field (mounting options) for the /var partition.
Example:
<device> /var <fstype> defaults,rw,nosuid,nodev,noexec,relatime 0 0
Run the following command to remount /var with the configured options:
# mount -o remount /var

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |

| | |
|---|---|
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |

| | |
|---|---|
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |

|  |  |
|---|---|
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
No matching files were found
```

## 1.1.2.5.2 Ensure nodev option set on /var/tmp partition

### Info

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

### Solution

- IF - a separate partition exists for /var/tmp
Edit the /etc/fstab file and add nodev to the fourth field (mounting options) for the /var/tmp partition.
Example:
<device> /var/tmp <fstype> defaults,rw,nosuid,nodev,noexec,relatime 0 0
Run the following command to remount /var/tmp with the configured options:
# mount -o remount /var/tmp

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |

| | |
|---|---|
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |

| | |
|---|---|
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |

| | |
|---|---|
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
No matching files were found
```

## 1.1.2.5.3 Ensure nosuid option set on /var/tmp partition

### Info

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

### Solution

- IF - a separate partition exists for /var/tmp
Edit the /etc/fstab file and add nosuid to the fourth field (mounting options) for the /var/tmp partition.
Example:
<device> /var/tmp <fstype> defaults,rw,nosuid,nodev,noexec,relatime 0 0
Run the following command to remount /var/tmp with the configured options:
# mount -o remount /var/tmp

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |

| | |
|---|---|
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |

| | |
|---|---|
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |

|  |  |
|---|---|
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
No matching files were found
```

## 1.1.2.5.4 Ensure noexec option set on /var/tmp partition

### Info

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

### Solution

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

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

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

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

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |

| | |
|---|---|
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |

| | |
|---|---|
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |

|  |  |
|---|---|
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
No matching files were found
```

## 1.1.2.6.2 Ensure nodev option set on /var/log partition

### Info

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

### Solution

- IF - a separate partition exists for /var/log
Edit the /etc/fstab file and add nodev to the fourth field (mounting options) for the /var/log partition.
Example:
<device> /var/log <fstype> defaults,rw,nosuid,nodev,noexec,relatime 0 0
Run the following command to remount /var/log with the configured options:
# mount -o remount /var/log

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |

| | |
|---|---|
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |

| | |
|---|---|
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |

| | |
|---|---|
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
No matching files were found
```

## 1.1.2.6.3 Ensure nosuid option set on /var/log partition

### Info

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

### Solution

- IF - a separate partition exists for /var/log
Edit the /etc/fstab file and add nosuid to the fourth field (mounting options) for the /var/log partition.
Example:
<device> /var/log <fstype> defaults,rw,nosuid,nodev,noexec,relatime 0 0
Run the following command to remount /var/log with the configured options:
# mount -o remount /var/log

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |

| | |
|---|---|
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |

| | |
|---|---|
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |

| | |
|---|---|
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
No matching files were found
```

## 1.1.2.6.4 Ensure noexec option set on /var/log partition

### Info

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

### Solution

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

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

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

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

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |

| | |
|---|---|
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |

| | |
|---|---|
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |

| | |
|---|---|
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
No matching files were found
```

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

### Info

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

### Solution

- IF - a separate partition exists for /var/log/audit
Edit the /etc/fstab file and add nodev to the fourth field (mounting options) for the /var/log/audit partition.
Example:
<device> /var/log/audit <fstype> defaults,rw,nosuid,nodev,noexec,relatime 0 0
Run the following command to remount /var/log/audit with the configured options:
# mount -o remount /var/log/audit

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |

| | |
|---|---|
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |

| | |
|---|---|
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |

|  |  |
|---|---|
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
No matching files were found
```

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

### Info

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

### Solution

- IF - a separate partition exists for /var/log/audit
Edit the /etc/fstab file and add nosuid to the fourth field (mounting options) for the /var/log/audit partition.
Example:
<device> /var/log/audit <fstype> defaults,rw,nosuid,nodev,noexec,relatime 0 0
Run the following command to remount /var/log/audit with the configured options:
# mount -o remount /var/log/audit

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |

| | |
|---|---|
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |

| | |
|---|---|
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |

|  |  |
|---|---|
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
No matching files were found
```

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

### Info

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

### Solution

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

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

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

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

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |

| | |
|---|---|
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |

| | |
|---|---|
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |

|  |  |
|---|---|
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
No matching files were found
```

## 1.3.1.3 Ensure all AppArmor Profiles are in enforce or complain mode

### Info

AppArmor profiles define what resources applications are able to access.
Security configuration requirements vary from site to site. Some sites may mandate a policy that is stricter than the default policy, which is perfectly acceptable. This item is intended to ensure that any policies that exist on the system are activated.

### Solution

Run the following command to set all profiles to enforce mode:
# aa-enforce /etc/apparmor.d/*
- OR -
Run the following command to set all profiles to complain mode:
# aa-complain /etc/apparmor.d/*
Note: Any unconfined processes may need to have a profile created or activated for them and then be restarted.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |

| | |
|---|---|
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |

| | |
|---|---|
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |

| | |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
 All of the following must pass to satisfy this requirement:

-------------------------
PASSED - apparmor_status - processes are confined
The command '/sbin/apparmor_status' returned :

apparmor module is loaded.
121 profiles are loaded.
26 profiles are in enforce mode.
   /usr/bin/man
   /usr/lib/snapd/snap-confine
   /usr/lib/snapd/snap-confine//mount-namespace-capture-helper
   /usr/sbin/mysqld
   docker-default
   lsb_release
   man_filter
   man_groff
   nvidia_modprobe
   nvidia_modprobe//kmod
   plasmashell
   plasmashell//QtWebEngineProcess
   rsyslogd
   tcpdump
   ubuntu_pro_apt_news
   ubuntu_pro_esm_cache
   ubuntu_pro_esm_cache//apt_methods
   ubuntu_pro_esm_cache//apt_methods_gpgv
   ubuntu_pro_esm_cache//cloud_id
   ubuntu_pro_esm_cache//dpkg
   ubuntu_pro_esm_cache//ps
   ubuntu_pro_esm_cache//ubuntu_distro_info
   ubuntu_pro_esm_cache_systemctl
   ubuntu_pro_esm_cache_systemd_detect_virt
   unix-chkpwd
   unprivileged_userns
4 profiles are in complain mode.
   transmission-cli
   transmission-daemon
   transmission-gtk
   transmission-qt
0 profiles are in prompt mode.
0 profiles are in kill mode.
91 profiles are in unconfined mode.
   1password
   Discord
   MongoDB Compass
   QtWebEngineProcess
   balena-etcher
   brave
   buildah
   busybox
   cam
   ch-checkns
   ch-run
   chrome
   crun
   devhelp
   element-desktop
   epiphany
   evolution
```

```
firefox
flatpak
foliate
geary
github-desktop
goldendict
ipa_verify
kchmviewer
keybase
lc-compliance
libcamerify
linux-sandbox
loupe
lxc-attach
lxc-create
lxc-destroy
lxc-execute
lxc-stop
lxc-unshare
lxc-usernsexec
mmdebstrap
msedge
nautilus
notepadqq
obsidian
opam
opera
pageedit
podman
polypane
privacybrowser
qcam
qmapshack
qutebrowser
rootlesskit
rpm
rssguard
runc
sbuild
sbuild-abort
sbuild-adduser
sbuild-apt
sbuild-checkpackages
sbuild-clean
sbuild-createchroot
sbuild-destroychroot
sbuild-distupgrade
[...]
```

## 1.4.2 Ensure access to bootloader config is configured

### Info

The grub configuration file contains information on boot settings and passwords for unlocking boot options.
Setting the permissions to read and write for root only prevents non-root users from seeing the boot parameters or changing them. Non-root users who read the boot parameters may be able to identify weaknesses in security upon boot and be able to exploit them.

### Solution

Run the following commands to set permissions on your grub configuration:

```
# chown root:root /boot/grub/grub.cfg # chmod u-x,go-rwx /boot/grub/grub.cfg
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |

| | |
|---|---|
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |

| | |
|---|---|
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |

|  |  |
|---|---|
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The file /boot/grub/grub.cfg with fmode owner: root group: root mode: 0600 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/boot/grub/grub.cfg
```

## 1.5.2 Ensure ptrace_scope is restricted

### Info

The ptrace() system call provides a means by which one process (the "tracer") may observe and control the execution of another process (the "tracee"), and examine and change the tracee's memory and registers.
The sysctl settings (writable only with CAP_SYS_PTRACE) are:
- 0 - classic ptrace permissions: a process can PTRACE_ATTACH to any other process running under the same uid, as long as it is dumpable (i.e. did not transition uids, start privileged, or have called prctl(PR_SET_DUMPABLE...) already). Similarly, PTRACE_TRACEME is unchanged.
- 1 - restricted ptrace: a process must have a predefined relationship with the inferior it wants to call PTRACE_ATTACH on. By default, this relationship is that of only its descendants when the above classic criteria is also met. To change the relationship, an inferior can call prctl(PR_SET_PTRACER, debugger, ...) to declare an allowed debugger PID to call PTRACE_ATTACH on the inferior. Using PTRACE_TRACEME is unchanged.
- 2 - admin-only attach: only processes with CAP_SYS_PTRACE may use ptrace with PTRACE_ATTACH, or through children calling PTRACE_TRACEME.
- 3 - no attach: no processes may use ptrace with PTRACE_ATTACH nor via PTRACE_TRACEME. Once set, this sysctl value cannot be changed.
If one application is compromised, it would be possible for an attacker to attach to other running processes (e.g. Bash, Firefox, SSH sessions, GPG agent, etc) to extract additional credentials and continue to expand the scope of their attack.
Enabling restricted mode will limit the ability of a compromised process to PTRACE_ATTACH on other processes running under the same user. With restricted mode, ptrace will continue to work with root user.

### Solution

Set the kernel.yama.ptrace_scope parameter in /etc/sysctl.conf or a file in /etc/sysctl.d/ ending inconf to a value of 1 2 or 3 :
kernel.yama.ptrace_scope = 1
- OR - kernel.yama.ptrace_scope = 2
- OR - kernel.yama.ptrace_scope = 3
Example:
# printf "%s " "kernel.yama.ptrace_scope = 1" >> /etc/sysctl.d/60-kernel_sysctl.conf
Run the following command to set the active kernel parameter:
# sysctl -w kernel.yama.ptrace_scope=1
Note:
- If a value of 2 or 3 is preferred, or required by local site policy, replace the 1 with the desired value of 2 or 3 in the example above
- If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |

|  |  |
|---|---|
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **
 - "kernel.yama.ptrace_scope" is correctly set to "1"
    in the running configuration
 - "kernel.yama.ptrace_scope" is correctly set to "1"
    in "/etc/sysctl.d/10-ptrace.conf"
```

## 1.5.4 Ensure prelink is not installed

### Info

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

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

### Solution

Run the following command to restore binaries to normal:

```
# prelink -ua
```

Uninstall prelink using the appropriate package manager or manual installation:

```
# apt purge prelink
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.7 |
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171R3** | 03.01.07b. |
| **800-171R3** | 03.03.01 |
| **800-171R3** | 03.03.03 |
| **800-53** | AC-6(9) |
| **800-53** | AU-2 |
| **800-53** | AU-12 |
| **800-53R5** | AC-6(9) |
| **800-53R5** | AU-2 |
| **800-53R5** | AU-12 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.3(a) |
| **CN-L3** | 8.1.10.6(a) |
| **CSCV7** | 14.9 |
| **CSCV8** | 3.14 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | DE.CM-7 |

| | |
|---|---|
| **CSF** | PR.AC-4 |
| **CSF** | PR.PT-1 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.PS-04 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.15 |
| **ISO-27001-2022** | A.8.18 |
| **ISO/IEC-27001** | A.12.4.3 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | AU-2 |
| **ITSG-33** | AU-12 |
| **LEVEL** | 1A |
| **NESA** | M1.2.2 |
| **NESA** | M5.5.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.5.4 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM7 |
| **NIAV2** | AM11a |
| **NIAV2** | AM11b |
| **NIAV2** | AM11c |

| | |
|---|---|
| **NIAV2** | AM11d |
| **NIAV2** | AM11e |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS30 |
| **NIAV2** | VL8 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV3.2.1** | 10.1 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **SWIFT-CSCV1** | 6.4 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The command '/bin/dpkg -s prelink 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'prelink' is not installed and no information is available
```

## 1.6.1 Ensure message of the day is configured properly

### Info

The contents of the /etc/motd file are displayed to users after login and function as a message of the day for authenticated users.
Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If mingetty(8) supports the following options, they display operating system information: m - machine architecture r - operating system release s - operating system name v - operating system version
Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " uname -a " command once they have logged in.

### Solution

Edit the /etc/motd file with the appropriate contents according to your site policy, remove any instances of m r s v or references to the OS platform
- OR -
- IF - the motd is not used, this file can be removed.
Run the following command to remove the motd file:
# rm /etc/motd

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.9 |
| **800-171R3** | 03.01.09 |
| **800-53** | AC-8a. |
| **800-53R5** | AC-8a. |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.5 |
| **ITSG-33** | AC-8a. |
| **LEVEL** | 1A |
| **NESA** | M5.2.5 |
| **NESA** | T5.5.1 |
| **NIAV2** | AM10a |
| **NIAV2** | AM10b |
| **NIAV2** | AM10c |
| **NIAV2** | AM10d |
| **NIAV2** | AM10e |
| **TBA-FIISB** | 45.2.4 |

### Assets

**linux_project**

## 1.6.4 Ensure access to /etc/motd is configured

### Info

The contents of the /etc/motd file are displayed to users after login and function as a message of the day for authenticated users.
- IF - the /etc/motd file does not have the correct access configured, it could be modified by unauthorized users with incorrect or misleading information.

### Solution

Run the following commands to set mode, owner, and group on /etc/motd :
# chown root:root $(readlink -e /etc/motd) # chmod u-x,go-wx $(readlink -e /etc/motd)
- OR -
Run the following command to remove the /etc/motd file:
# rm /etc/motd

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |

| | |
|---|---|
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |

| | |
|---|---|
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |

| | |
|---|---|
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

**Assets**

**linux_project**

## 1.6.5 Ensure access to /etc/issue is configured

### Info

The contents of the /etc/issue file are displayed to users prior to login for local terminals.
- IF - the /etc/issue file does not have the correct access configured, it could be modified by unauthorized users with incorrect or misleading information.

### Solution

Run the following commands to set mode, owner, and group on /etc/issue :
# chown root:root $(readlink -e /etc/issue) # chmod u-x,go-wx $(readlink -e /etc/issue)

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |

| | |
|---|---|
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |

| | |
|---|---|
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |

|  |  |
|---|---|
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The file /etc/issue with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/issue
```

## 1.6.6 Ensure access to /etc/issue.net is configured

### Info

The contents of the /etc/issue.net file are displayed to users prior to login for remote connections from configured services.
- IF - the /etc/issue.net file does not have the correct access configured, it could be modified by unauthorized users with incorrect or misleading information.

### Solution

Run the following commands to set mode, owner, and group on /etc/issue.net :
# chown root:root $(readlink -e /etc/issue.net) # chmod u-x,go-wx $(readlink -e /etc/issue.net)

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |

| | |
|---|---|
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |

| | |
|---|---|
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |

|  |  |
|---|---|
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The file /etc/issue.net with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/issue.net
```

## 1.7.10 Ensure XDMCP is not enabled

### Info

X Display Manager Control Protocol (XDMCP) is designed to provide authenticated access to display management services for remote displays
XDMCP is inherently insecure.
- XDMCP is not a ciphered protocol. This may allow an attacker to capture keystrokes entered by a user
- XDMCP is vulnerable to man-in-the-middle attacks. This may allow an attacker to steal the credentials of legitimate users by impersonating the XDMCP server.

### Solution

Edit all files returned by the audit and remove or commend out the Enable=true line in the [xdmcp] block:
Example file:
# GDM configuration storage # # See /usr/share/gdm/gdm.schemas for a list of available options.
[daemon] # Uncomment the line below to force the login screen to use Xorg #WaylandEnable=false
# Enabling automatic login # AutomaticLoginEnable = true # AutomaticLogin = user1
# Enabling timed login # TimedLoginEnable = true # TimedLogin = user1 # TimedLoginDelay = 10
[security]
[xdmcp] # Enable=true <- **This line should be removed or commented out**
[chooser]
[debug] # Uncomment the line below to turn on debugging # More verbose logs # Additionally lets the X server dump core if it crashes #Enable=true

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |

|  |  |
|---|---|
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

Pass
```

## 1.7.2 Ensure GDM login banner is configured

### Info

GDM is the GNOME Display Manager which handles graphical login for GNOME based systems.
Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place.

### Solution

- IF - A user profile is already created run the following commands to set and enable the text banner message on the login screen:
# gsettings set org.gnome.login-screen banner-message-text 'Authorized uses only. All activity may be monitored and reported' # gsettings set org.gnome.login-screen banner-message-enable true
Note:
- banner-message-text may be set in accordance with local site policy
- gsettings commands in this section MUST be done from a command window on a graphical desktop or an error will be returned.
- The system must be restarted after all gsettings configurations have been set in order for CIS-CAT Assessor to appropriately assess.
- OR/IF - A user profile does not exist:
- Create or edit the gdm profile in the /etc/dconf/profile/gdm with the following lines:
user-db:user system-db:gdm file-db:/usr/share/gdm/greeter-dconf-defaults
Note: gdm is the name of a dconf database.
<xhtml:ol start="2"> - Create a gdm keyfile for machine-wide settings in /etc/dconf/db/gdm.d/01-banner-message :
[org/gnome/login-screen] banner-message-enable=true banner-message-text='Type the banner message here.'
<xhtml:ol start="3"> - Update the system databases
# dconf update
Note:
- Users must log out and back in again before the system-wide settings take effect.
- There is no character limit for the banner message. gnome-shell autodetects longer stretches of text and enters two column mode.
- The banner message cannot be read from an external file.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.9 |
| **800-171R3** | 03.01.09 |
| **800-53** | AC-8 |
| **800-53R5** | AC-8 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.5 |
| **ITSG-33** | AC-8 |
| **LEVEL** | 1A |
| **NESA** | M1.3.6 |
| **TBA-FIISB** | 45.2.4 |

### Assets

**linux_project**

## 1.7.3 Ensure GDM disable-user-list option is enabled

### Info

GDM is the GNOME Display Manager which handles graphical login for GNOME based systems.
The disable-user-list option controls if a list of users is displayed on the login screen
Displaying the user list eliminates half of the Userid/Password equation that an unauthorized person would need to log on.

### Solution

- IF - A user profile exists run the following command to enable the disable-user-list :
# gsettings set org.gnome.login-screen disable-user-list true
Note:
- gsettings commands in this section MUST be done from a command window on a graphical desktop or an error will be returned.
- The system must be restarted after all gsettings configurations have been set in order for CIS-CAT Assessor to appropriately assess.
- OR/IF - A user profile does not exist:
- Create or edit the gdm profile in /etc/dconf/profile/gdm with the following lines:
user-db:user system-db:gdm file-db:/usr/share/gdm/greeter-dconf-defaults
Note: gdm is the name of a dconf database.
<xhtml:ol start="2"> - Create a gdm keyfile for machine-wide settings in /etc/dconf/db/gdm.d/00-login-screen : [org/gnome/login-screen] # Do not show the user list disable-user-list=true <xhtml:ol start="3"> - Update the system databases:
# dconf update
Note: When the user profile is created or changed, the user will need to log out and log in again before the changes will be applied.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.11 |
| **800-171R3** | 03.05.11 |
| **800-53** | IA-6 |
| **800-53R5** | IA-6 |
| **CSF2.0** | PR.AA-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.8.5 |
| **ITSG-33** | IA-6 |
| **ITSG-33** | IA-6a. |
| **LEVEL** | 1A |
| **NESA** | T5.5.1 |
| **QCSC-V1** | 13.2 |

### Assets

**linux_project**

## 1.7.4 Ensure GDM screen locks when the user is idle

### Info

GNOME Desktop Manager can make the screen lock automatically whenever the user is idle for some amount of time.
Setting a lock-out value reduces the window of opportunity for unauthorized user access to another user's session that has been left unattended.

### Solution

- IF - A user profile is already created run the following commands to enable screen locks when the user is idle:
# gsettings set org.gnome.desktop.screensaver lock-delay 5 # gsettings set org.gnome.desktop.session idle-delay 900
Note:
- gsettings commands in this section MUST be done from a command window on a graphical desktop or an error will be returned.
- The system must be restarted after all gsettings configurations have been set in order for CIS-CAT Assessor to appropriately assess.
- OR/IF- A user profile does not exist:
- Create or edit the user profile in the /etc/dconf/profile/ and verify it includes the following:
user-db:user system-db:{NAME_OF_DCONF_DATABASE}
Note: local is the name of a dconf database used in the examples.
<xhtml:ol start="2"> -
Create the directory /etc/dconf/db/local.d/ if it doesn't already exist:
-
Create the key file /etc/dconf/db/local.d/00-screensaver to provide information for the local database:
Example key file:
# Specify the dconf path [org/gnome/desktop/session]
# Number of seconds of inactivity before the screen goes blank # Set to 0 seconds if you want to deactivate the screensaver.
idle-delay=uint32 180
# Specify the dconf path [org/gnome/desktop/screensaver]
# Number of seconds after the screen is blank before locking the screen lock-delay=uint32 0
Note: You must include the uint32 along with the integer key values as shown.
<xhtml:ol start="4"> - Run the following command to update the system databases:
# dconf update <xhtml:ol start="5"> - Users must log out and back in again before the system-wide settings take effect.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.10 |
| **800-171** | 3.1.11 |
| **800-171R3** | 03.01.01h. |
| **800-171R3** | 03.01.10 |
| **800-171R3** | 03.01.11 |
| **800-53** | AC-2(5) |
| **800-53** | AC-11 |
| **800-53** | AC-11(1) |
| **800-53** | AC-12 |
| **800-53R5** | AC-2(5) |
| **800-53R5** | AC-11 |

| | |
|---|---|
| **800-53R5** | AC-11(1) |
| **800-53R5** | AC-12 |
| **CN-L3** | 7.1.2.2(d) |
| **CN-L3** | 7.1.3.2(d) |
| **CN-L3** | 7.1.3.7(b) |
| **CN-L3** | 8.1.4.1(b) |
| **CSCV7** | 16.11 |
| **CSCV8** | 4.3 |
| **CSF** | PR.AC-1 |
| **CSF** | PR.AC-4 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **HIPAA** | 164.312(a)(2)(iii) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.18 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.8.1 |
| **ISO-27001-2022** | A.8.2 |
| **ISO/IEC-27001** | A.9.2.1 |
| **ISO/IEC-27001** | A.11.2.8 |
| **ITSG-33** | AC-2(5) |
| **ITSG-33** | AC-11 |
| **ITSG-33** | AC-11(1) |
| **ITSG-33** | AC-12 |

| | |
|---|---|
| **LEVEL** | 1A |
| **NIAV2** | AM23c |
| **NIAV2** | AM23d |
| **NIAV2** | AM28 |
| **NIAV2** | NS5j |
| **NIAV2** | NS49 |
| **NIAV2** | SS14e |
| **PCI-DSSV3.2.1** | 8.1.8 |
| **PCI-DSSV4.0** | 8.2.8 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 13.2 |
| **QCSC-V1** | 15.2 |
| **TBA-FIISB** | 36.2.1 |
| **TBA-FIISB** | 37.1.4 |

| **Assets** |
|---|
| **linux_project** |

## 1.7.5 Ensure GDM screen locks cannot be overridden

### Info

GNOME Desktop Manager can lock down specific settings by using the lockdown mode in dconf to prevent users from changing specific settings.
To lock down a dconf key or subpath, create a locks subdirectory in the keyfile directory. The files inside this directory contain a list of keys or subpaths to lock. Just as with the keyfiles, you may add any number of files to this directory.
Setting a lock-out value reduces the window of opportunity for unauthorized user access to another user's session that has been left unattended.
Without locking down the system settings, user settings take precedence over the system settings.

### Solution

- To prevent the user from overriding these settings, create the file /etc/dconf/db/local.d/locks/00-screensaver with the following content:
# Lock desktop screensaver settings /org/gnome/desktop/session/idle-delay /org/gnome/desktop/screensaver/lock-delay <xhtml:ol start="2"> - Update the system databases:
# dconf update
Note:
- A user profile must exist in order to apply locks.
- Users must log out and back in again before the system-wide settings take effect.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.10 |
| **800-171** | 3.1.11 |
| **800-171R3** | 03.01.01h. |
| **800-171R3** | 03.01.10 |
| **800-171R3** | 03.01.11 |
| **800-53** | AC-2(5) |
| **800-53** | AC-11 |
| **800-53** | AC-11(1) |
| **800-53** | AC-12 |
| **800-53R5** | AC-2(5) |
| **800-53R5** | AC-11 |
| **800-53R5** | AC-11(1) |
| **800-53R5** | AC-12 |
| **CN-L3** | 7.1.2.2(d) |
| **CN-L3** | 7.1.3.2(d) |
| **CN-L3** | 7.1.3.7(b) |
| **CN-L3** | 8.1.4.1(b) |
| **CSCV7** | 16.11 |

| | |
|---|---|
| **CSCV8** | 4.3 |
| **CSF** | PR.AC-1 |
| **CSF** | PR.AC-4 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **HIPAA** | 164.312(a)(2)(iii) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.18 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.8.1 |
| **ISO-27001-2022** | A.8.2 |
| **ISO/IEC-27001** | A.9.2.1 |
| **ISO/IEC-27001** | A.11.2.8 |
| **ITSG-33** | AC-2(5) |
| **ITSG-33** | AC-11 |
| **ITSG-33** | AC-11(1) |
| **ITSG-33** | AC-12 |
| **LEVEL** | 1A |
| **NIAV2** | AM23c |
| **NIAV2** | AM23d |
| **NIAV2** | AM28 |
| **NIAV2** | NS5j |
| **NIAV2** | NS49 |
| **NIAV2** | SS14e |

|  |  |
|---|---|
| **PCI-DSSV3.2.1** | 8.1.8 |
| **PCI-DSSV4.0** | 8.2.8 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 13.2 |
| **QCSC-V1** | 15.2 |
| **TBA-FIISB** | 36.2.1 |
| **TBA-FIISB** | 37.1.4 |

**Assets**

**linux_project**

## 1.7.6 Ensure GDM automatic mounting of removable media is disabled

### Info

By default GNOME automatically mounts removable media when inserted as a convenience to the user.
With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.

### Solution

- IF - A user profile exists run the following commands to ensure automatic mounting is disabled:
# gsettings set org.gnome.desktop.media-handling automount false # gsettings set org.gnome.desktop.media-handling automount-open false
Note:
- gsettings commands in this section MUST be done from a command window on a graphical desktop or an error will be returned.
- The system must be restarted after all gsettings configurations have been set in order for CIS-CAT Assessor to appropriately assess.
- OR/IF - A user profile does not exist:
- Create a file /etc/dconf/db/local.d/00-media-automount with following content:
[org/gnome/desktop/media-handling] automount=false automount-open=false <xhtml:ol start="2"> - After creating the file, apply the changes using below command :
# dconf update
Note: Users must log out and back in again before the system-wide settings take effect.
Impact:
The use of portable hard drives is very common for workstation users. If your organization allows the use of portable storage or media on workstations and physical access controls to workstations is considered adequate there is little value add in turning off automounting.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.8.7 |
| **800-171R3** | 03.08.07 |
| **800-53** | MP-7 |
| **800-53R5** | MP-7 |
| **CN-L3** | 8.5.4.1(c) |
| **CSCV7** | 8.5 |
| **CSCV8** | 10.3 |
| **CSF** | PR.PT-2 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.7.10 |
| **ISO/IEC-27001** | A.8.3.1 |
| **ISO/IEC-27001** | A.8.3.3 |
| **LEVEL** | 1A |

| | |
|---|---|
| **NESA** | T1.4.1 |

**Assets**

**linux_project**

## 1.7.7 Ensure GDM disabling automatic mounting of removable media is not overridden

### Info

By default GNOME automatically mounts removable media when inserted as a convenience to the user.
By using the lockdown mode in dconf, you can prevent users from changing specific settings. To lock down a dconf key or subpath, create a locks subdirectory in the keyfile directory. The files inside this directory contain a list of keys or subpaths to lock. Just as with the keyfiles, you may add any number of files to this directory.
With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.

### Solution

- To prevent the user from overriding these settings, create the file /etc/dconf/db/local.d/locks/00-media-automount with the following content:
[org/gnome/desktop/media-handling] automount=false automount-open=false <xhtml:ol start="2"> - Update the systems databases:
# dconf update
Note:
- A user profile must exist in order to apply locks.
- Users must log out and back in again before the system-wide settings take effect.
Impact:
The use of portable hard drives is very common for workstation users

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.08.02 |
| **800-53** | MP-2 |
| **800-53R5** | MP-2 |
| **CSF** | PR.PT-2 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |

| Assets |
|---|
| **linux_project** |

## 1.7.8 Ensure GDM autorun-never is enabled

### Info

The autorun-never setting allows the GNOME Desktop Display Manager to disable autorun through GDM.
Malware on removable media may taking advantage of Autorun features when the media is inserted into a system and execute.

### Solution

- IF - A user profile exists run the following command to set autorun-never to true for GDM users:
# gsettings set org.gnome.desktop.media-handling autorun-never true
Note:
- gsettings commands in this section MUST be done from a command window on a graphical desktop or an error will be returned.
- The system must be restarted after all gsettings configurations have been set in order for CIS-CAT Assessor to appropriately assess.
- OR/IF - A user profile does not exist:
- create the file /etc/dconf/db/local.d/locks/00-media-autorun with the following content:
[org/gnome/desktop/media-handling] autorun-never=true <xhtml:ol start="2"> - Update the systems databases:
# dconf update
Note: Users must log out and back in again before the system-wide settings take effect.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.8.7 |
| **800-171R3** | 03.08.07 |
| **800-53** | MP-7 |
| **800-53R5** | MP-7 |
| **CN-L3** | 8.5.4.1(c) |
| **CSCV7** | 8.5 |
| **CSCV8** | 10.3 |
| **CSF** | PR.PT-2 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.7.10 |
| **ISO/IEC-27001** | A.8.3.1 |
| **ISO/IEC-27001** | A.8.3.3 |
| **LEVEL** | 1A |
| **NESA** | T1.4.1 |

### Assets

**linux_project**

## 1.7.9 Ensure GDM autorun-never is not overridden

### Info

The autorun-never setting allows the GNOME Desktop Display Manager to disable autorun through GDM.
By using the lockdown mode in dconf, you can prevent users from changing specific settings.
To lock down a dconf key or subpath, create a locks subdirectory in the keyfile directory. The files inside this directory contain a list of keys or subpaths to lock. Just as with the keyfiles, you may add any number of files to this directory.
Malware on removable media may taking advantage of Autorun features when the media is inserted into a system and execute.

### Solution

- To prevent the user from overriding these settings, create the file /etc/dconf/db/local.d/locks/00-media-autorun with the following content:
[org/gnome/desktop/media-handling] autorun-never=true <xhtml:ol start="2"> - Update the systems databases:
# dconf update
Note:
- A user profile must exist in order to apply locks.
- Users must log out and back in again before the system-wide settings take effect.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.8.7 |
| **800-171R3** | 03.08.07 |
| **800-53** | MP-7 |
| **800-53R5** | MP-7 |
| **CN-L3** | 8.5.4.1(c) |
| **CSCV7** | 8.5 |
| **CSCV8** | 10.3 |
| **CSF** | PR.PT-2 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.7.10 |
| **ISO/IEC-27001** | A.8.3.1 |
| **ISO/IEC-27001** | A.8.3.3 |
| **LEVEL** | 1A |
| **NESA** | T1.4.1 |

### Assets

**linux_project**

## 2.1.1 Ensure autofs services are not in use

### Info

autofs allows automatic mounting of devices, typically including CD/DVDs and USB drives.
With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in the filesystem even if they lacked permissions to mount it themselves.

### Solution

Run the following commands to stop autofs.service and remove the autofs package:
# systemctl stop autofs.service # apt purge autofs
- OR -
- IF - the autofs package is required as a dependency:
Run the following commands to stop and mask autofs.service :
# systemctl stop autofs.service # systemctl mask autofs.service
Impact:
The use of portable hard drives is very common for workstation users. If your organization allows the use of portable storage or media on workstations and physical access controls to workstations is considered adequate there is little value add in turning off automounting.
There may be packages that are dependent on the autofs package. If the autofs package is removed, these dependent packages will be removed as well. Before removing the autofs package, review any dependent packages to determine if they are required on the system.
- IF - a dependent package is required: stop and mask the autofs.service leaving the autofs package installed.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.8.7 |
| **800-171R3** | 03.08.07 |
| **800-53** | MP-7 |
| **800-53R5** | MP-7 |
| **CN-L3** | 8.5.4.1(c) |
| **CSCV7** | 8.5 |
| **CSCV8** | 10.3 |
| **CSF** | PR.PT-2 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.7.10 |
| **ISO/IEC-27001** | A.8.3.1 |
| **ISO/IEC-27001** | A.8.3.3 |
| **LEVEL** | 1A |
| **NESA** | T1.4.1 |

### Assets

**linux_project**

```
The command '/bin/dpkg -s autofs 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'autofs' is not installed and no information is available
```

## 2.1.10 Ensure nis server services are not in use

### Info

The Network Information Service (NIS) (formally known as Yellow Pages) is a client-server directory service protocol for distributing system configuration files. The NIS server is a collection of programs that allow for the distribution of configuration files. The NIS client ( ypbind ) was used to bind a machine to an NIS server and receive the distributed configuration files.
ypserv.service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that ypserv.service be removed and other, more secure services be used

### Solution

Run the following commands to stop ypserv.service and remove ypserv package:
# systemctl stop ypserv.service # apt purge ypserv
- OR -
- IF - the ypserv package is required as a dependency:
Run the following commands to stop and mask ypserv.service :
# systemctl stop ypserv.service # systemctl mask ypserv.service
Impact:
There may be packages that are dependent on the ypserv package. If the ypserv package is removed, these dependent packages will be removed as well. Before removing the ypserv package, review any dependent packages to determine if they are required on the system.
- IF - a dependent package is required: stop and mask the ypserv.service leaving the ypserv package installed.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |

| | |
|---|---|
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command '/bin/dpkg -s ypserv 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'ypserv' is not installed and no information is available
```

## 2.1.11 Ensure print server services are not in use

### Info

The Common Unix Print System (CUPS) provides the ability to print to both local and network printers. A system running CUPS can also accept print jobs from remote systems and print them to local printers. It also provides a web based remote administration capability.
If the system does not need to print jobs or accept print jobs from other systems, it is recommended that CUPS be removed to reduce the potential attack surface.

### Solution

Run the following commands to stop cups.socket and cups.service and remove the cups package:
# systemctl stop cups.socket cups.service # apt purge cups
- OR -
- IF - the cups package is required as a dependency:
Run the following commands to stop and mask the cups.socket and cups.service :
# systemctl stop cups.socket cups.service # systemctl mask cups.socket cups.service
Impact:
Removing the cups package, or disabling cups.socket and/or cups.service will prevent printing from the system, a common task for workstation systems.
There may be packages that are dependent on the cups package. If the cups package is removed, these dependent packages will be removed as well. Before removing the cups package, review any dependent packages to determine if they are required on the system.
- IF - a dependent package is required: stop and mask cups.socket and cups.service leaving the cups package installed.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |

|  |  |
|---|---|
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command '/bin/dpkg -s cups 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'cups' is not installed and no information is available
```

## 2.1.12 Ensure rpcbind services are not in use

### Info

The rpcbind utility maps RPC services to the ports on which they listen. RPC processes notify rpcbind when they start, registering the ports they are listening on and the RPC program numbers they expect to serve. The client system then contacts rpcbind on the server with a particular RPC program number. The rpcbind.service redirects the client to the proper port number so it can communicate with the requested service.
Portmapper is an RPC service, which always listens on tcp and udp 111, and is used to map other RPC services (such as nfs, nlockmgr, quotad, mountd, etc.) to their corresponding port number on the server. When a remote host makes an RPC call to that server, it first consults with portmap to determine where the RPC server is listening.
A small request (~82 bytes via UDP) sent to the Portmapper generates a large response (7x to 28x amplification), which makes it a suitable tool for DDoS attacks. If rpcbind is not required, it is recommended to remove rpcbind package to reduce the potential attack surface.

### Solution

Run the following commands to stop rpcbind.socket and rpcbind.service and remove the rpcbind package:
# systemctl stop rpcbind.socket rpcbind.service # apt purge rpcbind
- OR -
- IF - the rpcbind package is required as a dependency:
Run the following commands to stop and mask the rpcbind.socket and rpcbind.service :
# systemctl stop rpcbind.socket rpcbind.service # systemctl mask rpcbind.socket rpcbind.service
Impact:
Many of the libvirt packages used by Enterprise Linux virtualization, and the nfs-utils package used for The Network File System (NFS), are dependent on the rpcbind package. If the rpcbind package is removed, these dependent packages will be removed as well. Before removing the rpcbind package, review any dependent packages to determine if they are required on the system.
- IF - a dependent package is required: stop and mask the rpcbind.socket and rpcbind.service leaving the rpcbind package installed.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |

|  |  |
|---|---|
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command '/bin/dpkg -s rpcbind 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'rpcbind' is not installed and no information is available
```

## 2.1.13 Ensure rsync services are not in use

### Info

The rsync service can be used to synchronize files between systems over network links.
rsync.service presents a security risk as the rsync protocol is unencrypted.
The rsync package should be removed to reduce the attack area of the system.

### Solution

Run the following commands to stop rsync.service and remove the rsync package:
# systemctl stop rsync.service # apt purge rsync
- OR -
- IF - the rsync package is required as a dependency:
Run the following commands to stop and mask rsync.service :
# systemctl stop rsync.service # systemctl mask rsync.service
Impact:
There may be packages that are dependent on the rsync package. If the rsync package is removed, these dependent packages will be removed as well. Before removing the rsync package, review any dependent packages to determine if they are required on the system.
- IF - a dependent package is required: stop and mask rsync.service leaving the rsync package installed.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |

| | |
|---|---|
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - rsync not active
The command '/bin/systemctl is-active rsync.service 2>/dev/null | /bin/grep '^active' | /bin/awk
 '{print} END {if (NR == 0) print "pass" ; else print "fail"}'' returned :

pass

-------------------------
PASSED - rsync not enabled
The command '/bin/systemctl is-enabled rsync.service 2>/dev/null | /bin/grep '^enabled' | /bin/awk
 '{print} END {if (NR == 0) print "pass" ; else print "fail"}'' returned :

pass
```

## 2.1.14 Ensure samba file server services are not in use

### Info

The Samba daemon allows system administrators to configure their Linux systems to share file systems and directories with Windows desktops. Samba will advertise the file systems and directories via the Server Message Block (SMB) protocol. Windows desktop users will be able to mount these directories and file systems as letter drives on their systems.
If there is no need to mount directories and file systems to Windows systems, then this service should be deleted to reduce the potential attack surface.

### Solution

Run the following commands to stop smbd.service and remove samba package:

```
# systemctl stop smbd.service # apt purge samba
```

- OR -
- IF - the samba package is required as a dependency:
Run the following commands to stop and mask the smbd.service :

```
# systemctl stop smbd.service # systemctl mask smbd.service
```

Impact:
There may be packages that are dependent on the samba package. If the samba package is removed, these dependent packages will be removed as well. Before removing the samba package, review any dependent packages to determine if they are required on the system.
- IF - a dependent package is required: stop and mask the smbd.service leaving the samba package installed.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |

| | |
|---|---|
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command '/bin/dpkg -s samba 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'samba' is not installed and no information is available
```

## 2.1.15 Ensure snmp services are not in use

### Info

Simple Network Management Protocol (SNMP) is a widely used protocol for monitoring the health and welfare of network equipment, computer equipment and devices like UPSs.
Net-SNMP is a suite of applications used to implement SNMPv1 (RFC 1157), SNMPv2 (RFCs 1901-1908), and SNMPv3 (RFCs 3411-3418) using both IPv4 and IPv6.
Support for SNMPv2 classic (a.k.a. "SNMPv2 historic" - RFCs 1441-1452) was dropped with the 4.0 release of the UCD-snmp package.
The Simple Network Management Protocol (SNMP) server is used to listen for SNMP commands from an SNMP management system, execute the commands or collect the information and then send results back to the requesting system.
The SNMP server can communicate using SNMPv1 which transmits data in the clear and does not require authentication to execute commands. SNMPv3 replaces the simple/clear text password sharing used in SNMPv2 with more securely encoded parameters. If the the SNMP service is not required, the snmpd package should be removed to reduce the attack surface of the system.
Note: If SNMP is required:
- The server should be configured for SNMP v3 only. User Authentication and Message Encryption should be configured.
- If SNMP v2 is absolutely necessary, modify the community strings' values.

### Solution

Run the following commands to stop snmpd.service and remove the snmpd package:
# systemctl stop snmpd.service # apt purge snmpd
- OR - If the package is required for dependencies:
Run the following commands to stop and mask the snmpd.service :
# systemctl stop snmpd.service # systemctl mask snmpd.service
Impact:
There may be packages that are dependent on the snmpd package. If the snmpd package is removed, these packages will be removed as well.
Before removing the snmpd package, review any dependent packages to determine if they are required on the system. If a dependent package is required, stop and mask the snmpd.service leaving the snmpd package installed.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |

| | |
|---|---|
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command '/bin/dpkg -s snmpd 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'snmpd' is not installed and no information is available
```

## 2.1.16 Ensure tftp server services are not in use

### Info

Trivial File Transfer Protocol (TFTP) is a simple protocol for exchanging files between two TCP/IP machines. TFTP servers allow connections from a TFTP Client for sending and receiving files.
Unless there is a need to run the system as a TFTP server, it is recommended that the package be removed to reduce the potential attack surface.
TFTP does not have built-in encryption, access control or authentication. This makes it very easy for an attacker to exploit TFTP to gain access to files

### Solution

Run the following commands to stop tftpd-hpa.service and remove the tftpd-hpa package:
# systemctl stop tftpd-hpa.service # apt purge tftpd-hpa
- OR -
- IF - the tftpd-hpa package is required as a dependency:
Run the following commands to stop and mask tftpd-hpa.service :
# systemctl stop tftpd-hpa.service # systemctl mask tftpd-hpa.service
Impact:
TFTP is often used to provide files for network booting such as for PXE based installation of servers.
There may be packages that are dependent on the tftpd-hpa package. If the tftpd-hpa package is removed, these dependent packages will be removed as well. Before removing the tftpd-hpa package, review any dependent packages to determine if they are required on the system.
- IF - a dependent package is required: stop and mask tftpd-hpa.service leaving the tftpd-hpa package installed.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |

| | |
|---|---|
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command '/bin/dpkg -s tftpd-hpa 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'tftpd-hpa' is not installed and no information is available
```

## 2.1.17 Ensure web proxy server services are not in use

### Info

Squid is a standard proxy server used in many distributions and environments.
Unless a system is specifically set up to act as a proxy server, it is recommended that the squid package be removed to reduce the potential attack surface.
Note: Several HTTP proxy servers exist. These should be checked and removed unless required.

### Solution

Run the following commands to stop squid.service and remove the squid package:
# systemctl stop squid.service # apt purge squid
- OR - If the squid package is required as a dependency:
Run the following commands to stop and mask the squid.service :
# systemctl stop squid.service # systemctl mask squid.service
Impact:
There may be packages that are dependent on the squid package. If the squid package is removed, these dependent packages will be removed as well. Before removing the squid package, review any dependent packages to determine if they are required on the system.
- IF - a dependent package is required: stop and mask the squid.service leaving the squid package installed.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |

|  |  |
|---|---|
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

### Assets

### linux_project

```
The command '/bin/dpkg -s squid 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'squid' is not installed and no information is available
```

## 2.1.18 Ensure web server services are not in use

### Info

Web servers provide the ability to host web site content.
Unless there is a local site approved requirement to run a web server service on the system, web server packages should be removed to reduce the potential attack surface.

### Solution

Run the following commands to stop httpd.socket httpd.service and nginx.service and remove apache2 and nginx packages:
# systemctl stop apache2.socket apache2.service nginx.service # apt purge apache2 nginx
- OR -
- IF - a package is installed and is required for dependencies:
Run the following commands to stop and mask apache2.socket apache2.service and nginx.service :
# systemctl stop apache2.socket apache2.service nginx.service # systemctl mask apache2.socket apache2.service nginx.service
Note: Other web server packages may exist. If not required and authorized by local site policy, they should also be removed. If the package is required for a dependency, the service and socket should be stopped and masked.
Impact:
Removal of web server packages will remove that ability for the server to host web services.
- IF - the web server package is required for a dependency, any related service or socket should be stopped and masked.
Note: If the remediation steps to mask a service are followed and that package is not installed on the system, the service and/or socket will still be masked. If the package is installed due to an approved requirement to host a web server, the associated service and/or socket would need to be unmasked before it could be enabled and/or started.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |

|  |  |
|---|---|
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

**Assets**

**linux_project**

## 2.1.19 Ensure xinetd services are not in use

### Info

The eXtended InterNET Daemon ( xinetd ) is an open source super daemon that replaced the original inetd daemon. The xinetd daemon listens for well known services and dispatches the appropriate daemon to properly respond to service requests.
If there are no xinetd services required, it is recommended that the package be removed to reduce the attack surface are of the system.
Note: If an xinetd service or services are required, ensure that any xinetd service not required is stopped and masked

### Solution

Run the following commands to stop xinetd.service and remove the xinetd package:
# systemctl stop xinetd.service # apt purge xinetd
-OR-
-IF- the xinetd package is required as a dependency:
Run the following commands to stop and mask the xinetd.service :
# systemctl stop xinetd.service # systemctl mask xinetd.service
Impact:
There may be packages that are dependent on the xinetd package. If the xinetd package is removed, these dependent packages will be removed as well. Before removing the xinetd package, review any dependent packages to determine if they are required on the system.
-IF- a dependent package is required: stop and mask xinetd.service leaving the xinetd package installed.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |

| | |
|---|---|
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command '/bin/dpkg -s xinetd 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'xinetd' is not installed and no information is available
```

## 2.1.2 Ensure avahi daemon services are not in use

### Info

Avahi is a free zeroconf implementation, including a system for multicast DNS/DNS-SD service discovery. Avahi allows programs to publish and discover services and hosts running on a local network with no specific configuration. For example, a user can plug a computer into a network and Avahi automatically finds printers to print to, files to look at and people to talk to, as well as network services running on the machine.
Automatic discovery of network services is not normally required for system functionality. It is recommended to remove this package to reduce the potential attack surface.

### Solution

Run the following commands to stop avahi-daemon.socket and avahi-daemon.service and remove the avahi-daemon package:
# systemctl stop avahi-daemon.socket avahi-daemon.service # apt purge avahi-daemon
- OR -
- IF - the avahi-daemon package is required as a dependency:
Run the following commands to stop and mask the avahi-daemon.socket and avahi-daemon.service :
# systemctl stop avahi-daemon.socket avahi-daemon.service # systemctl mask avahi-daemon.socket avahi-daemon.service
Impact:
There may be packages that are dependent on the avahi package. If the avahi package is removed, these dependent packages will be removed as well. Before removing the avahi package, review any dependent packages to determine if they are required on the system.
- IF - a dependent package is required: stop and mask the avahi-daemon.socket and avahi-daemon.service leaving the avahi package installed.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |

| | |
|---|---|
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command '/bin/dpkg -s avahi-daemon 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'avahi-daemon' is not installed and no information is available
```

## 2.1.21 Ensure mail transfer agent is configured for local-only mode

### Info

Mail Transfer Agents (MTA), such as sendmail and Postfix, are used to listen for incoming mail and transfer the messages to the appropriate user or mail server. If the system is not intended to be a mail server, it is recommended that the MTA be configured to only process local mail.
The software for all Mail Transfer Agents is complex and most have a long history of security issues. While it is important to ensure that the system can process local mail messages, it is not necessary to have the MTA's daemon listening on a port unless the server is intended to be a mail server that receives and processes mail from other systems.

### Solution

Edit /etc/postfix/main.cf and add the following line to the RECEIVING MAIL section. If the line already exists, change it to look like the line below:
inet_interfaces = loopback-only
Run the following command to restart postfix :
# systemctl restart postfix
Note:
- This recommendation is designed around the postfix mail server.
- Depending on your environment you may have an alternative MTA installed such as exim4. If this is the case consult the documentation for your installed MTA to configure the recommended state.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |

|  |  |
|---|---|
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **
 - Port "25" is not listening on a non-loopback network interface
 - Port "465" is not listening on a non-loopback network interface
 - Port "587" is not listening on a non-loopback network interface
 - MTA not detected or in use
```

## 2.1.3 Ensure dhcp server services are not in use

### Info

The Dynamic Host Configuration Protocol (DHCP) is a service that allows machines to be dynamically assigned IP addresses. There are two versions of the DHCP protocol DHCPv4 and DHCPv6 At startup the server may be started for one or the other via the -4 or -6 arguments.
Unless a system is specifically set up to act as a DHCP server, it is recommended that this package be removed to reduce the potential attack surface.

### Solution

Run the following commands to stop isc-dhcp-server.service and isc-dhcp-server6.service and remove the isc-dhcp-server package:
# systemctl stop isc-dhcp-server.service isc-dhcp-server6.service # apt purge isc-dhcp-server
- OR -
- IF - the isc-dhcp-server package is required as a dependency:
Run the following commands to stop and mask isc-dhcp-server.service and isc-dhcp-server6.service :
# systemctl stop isc-dhcp-server.service isc-dhcp-server6.service # systemctl mask isc-dhcp-server isc-dhcp-server6.service
Impact:
There may be packages that are dependent on the isc-dhcp-server package. If the isc-dhcp-server package is removed, these dependent packages will be removed as well. Before removing the isc-dhcp-server package, review any dependent packages to determine if they are required on the system.
- IF - a dependent package is required: stop and mask the isc-dhcp-server.service and isc-dhcp-server6.service leaving the isc-dhcp-server package installed.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |

|  |  |
|---|---|
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command '/bin/dpkg -s isc-dhcp-server 2>&1 | /bin/grep -E '(^Status:|not installed)''
 returned :

dpkg-query: package 'isc-dhcp-server' is not installed and no information is available
```

## 2.1.4 Ensure dns server services are not in use

### Info

The Domain Name System (DNS) is a hierarchical naming system that maps names to IP addresses for computers, services and other resources connected to a network.
Note: bind9 is the package and bind.service is the alias for named.service
Unless a system is specifically designated to act as a DNS server, it is recommended that the package be deleted to reduce the potential attack surface.

### Solution

Run the following commands to stop named.service and remove the bind9 package:
# systemctl stop named.service # apt purge bind9
- OR -
- IF - the bind9 package is required as a dependency:
Run the following commands to stop and mask bind9.service :
# systemctl stop named.service # systemctl mask named.service
Impact:
There may be packages that are dependent on the bind9 package. If the bind9 package is removed, these dependent packages will be removed as well. Before removing the bind9 package, review any dependent packages to determine if they are required on the system.
- IF - a dependent package is required: stop and mask named.service leaving the bind9 package installed.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |

| | |
|---|---|
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command '/bin/dpkg -s bind9 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'bind9' is not installed and no information is available
```

## 2.1.5 Ensure dnsmasq services are not in use

### Info

dnsmasq is a lightweight tool that provides DNS caching, DNS forwarding and DHCP (Dynamic Host Configuration Protocol) services.
Unless a system is specifically designated to act as a DNS caching, DNS forwarding and/or DHCP server, it is recommended that the package be removed to reduce the potential attack surface.

### Solution

Run the following commands to stop dnsmasq.service and remove dnsmasq package:
# systemctl stop dnsmasq.service # apt purge dnsmasq
- OR -
- IF - the dnsmasq package is required as a dependency:
Run the following commands to stop and mask the dnsmasq.service :
# systemctl stop dnsmasq.service # systemctl mask dnsmasq.service
Impact:
There may be packages that are dependent on the dnsmasq package. If the dnsmasq package is removed, these dependent packages will be removed as well. Before removing the dnsmasq package, review any dependent packages to determine if they are required on the system.
- IF - a dependent package is required: stop and mask the dnsmasq.service leaving the dnsmasq package installed.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |

|  |  |
|---|---|
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command '/bin/dpkg -s dnsmasq 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'dnsmasq' is not installed and no information is available
```

## 2.1.6 Ensure ftp server services are not in use

### Info

The File Transfer Protocol (FTP) provides networked computers with the ability to transfer files. vsftpd is the Very Secure File Transfer Protocol Daemon.
FTP does not protect the confidentiality of data or authentication credentials. It is recommended SFTP be used if file transfer is required. Unless there is a need to run the system as a FTP server (for example, to allow anonymous downloads), it is recommended that the package be deleted to reduce the potential attack surface.

### Solution

Run the following commands to stop vsftpd.service and remove the vsftpd package:
# systemctl stop vsftpd.service # apt purge vsftpd
- OR -
- IF - the vsftpd package is required as a dependency:
Run the following commands to stop and mask the vsftpd.service :
# systemctl stop vsftpd.service # systemctl mask vsftpd.service
Note: Other ftp server packages may exist. If not required and authorized by local site policy, they should also be removed. If the package is required for a dependency, the service should be stopped and masked.
Impact:
There may be packages that are dependent on the vsftpd package. If the vsftpd package is removed, these dependent packages will be removed as well. Before removing the vsftpd package, review any dependent packages to determine if they are required on the system.
- IF - a dependent package is required: stop and mask the vsftpd.service leaving the vsftpd package installed.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |

| | |
|---|---|
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command '/bin/dpkg -s vsftpd 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'vsftpd' is not installed and no information is available
```

## 2.1.7 Ensure ldap server services are not in use

### Info

The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service that provides a method for looking up information from a central database.
If the system will not need to act as an LDAP server, it is recommended that the software be removed to reduce the potential attack surface.

### Solution

Run the following commands to stop slapd.service and remove the slapd package:
# systemctl stop slapd.service # apt purge slapd
- OR -
- IF - the slapd package is required as a dependency:
Run the following commands to stop and mask slapd.service :
# systemctl stop slapd.service # systemctl mask slapd.service
Impact:
There may be packages that are dependent on the slapd package. If the slapd package is removed, these dependent packages will be removed as well. Before removing the slapd package, review any dependent packages to determine if they are required on the system.
- IF - a dependent package is required: stop and mask the slapd.service leaving the slapd package installed.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |

| | |
|---|---|
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command '/bin/dpkg -s slapd 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'slapd' is not installed and no information is available
```

## 2.1.8 Ensure message access server services are not in use

### Info

dovecot-imapd and dovecot-pop3d are an open source IMAP and POP3 server for Linux based systems.
Unless POP3 and/or IMAP servers are to be provided by this system, it is recommended that the package be removed to reduce the potential attack surface.
Note: Several IMAP/POP3 servers exist and can use other service names. These should also be audited and the packages removed if not required.

### Solution

Run one of the following commands to remove dovecot-imapd and dovecot-pop3d :
Run the following commands to stop dovecot.socket and dovecot.service and remove the dovecot-imapd and dovecot-pop3d packages:
# systemctl stop dovecot.socket dovecot.service # apt purge dovecot-imapd dovecot-pop3d
- OR -
- IF - a package is installed and is required for dependencies:
Run the following commands to stop and mask dovecot.socket and dovecot.service :
# systemctl stop dovecot.socket dovecot.service # systemctl mask dovecot.socket dovecot.service
Impact:
There may be packages that are dependent on dovecot-imapd and/or dovecot-pop3d packages. If dovecot-imapd and dovecot-pop3d packages are removed, these dependent packages will be removed as well. Before removing dovecot-imapd and/or dovecot-pop3d packages, review any dependent packages to determine if they are required on the system.
- IF - a dependent package is required: stop and mask dovecot.socket and dovecot.service leaving dovecot-imapd and/or dovecot-pop3d packages installed.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |

|  |  |
|---|---|
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - dovecot-pop3 not installed
The command '/bin/dpkg -s dovecot-pop3 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'dovecot-pop3' is not installed and no information is available

-------------------------
PASSED - dovecot-imapd not installed
The command '/bin/dpkg -s dovecot-imapd 2>&1 | /bin/grep -E '(^Status:|not installed)''
 returned :

dpkg-query: package 'dovecot-imapd' is not installed and no information is available
```

## 2.1.9 Ensure network file system services are not in use

### Info

The Network File System (NFS) is one of the first and most widely distributed file systems in the UNIX environment. It provides the ability for systems to mount file systems of other servers through the network.
If the system does not export NFS shares, it is recommended that the nfs-kernel-server package be removed to reduce the remote attack surface.

### Solution

Run the following command to stop nfs-server.service and remove nfs-kernel-server package:
# systemctl stop nfs-server.service # apt purge nfs-kernel-server
- OR -
- IF - the nfs-kernel-server package is required as a dependency:
Run the following commands to stop and mask the nfs-server.service :
# systemctl stop nfs-server.service # systemctl mask nfs-server.service
Impact:
There may be packages that are dependent on the nfs-kernel-server package. If the nfs-kernel-server package is removed, these dependent packages will be removed as well. Before removing the nfs-kernel-server package, review any dependent packages to determine if they are required on the system.
- IF - a dependent package is required: stop and mask the nfs-server.service leaving the nfs-kernel-server package installed.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |

|  |  |
|---|---|
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command '/bin/dpkg -s nfs-kernel-server 2>&1 | /bin/grep -E '(^Status:|not installed)''
 returned :

dpkg-query: package 'nfs-kernel-server' is not installed and no information is available
```

## 2.2.1 Ensure NIS Client is not installed

### Info

The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client was used to bind a machine to an NIS server and receive the distributed configuration files.
The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed.

### Solution

Uninstall nis :
# apt purge nis
Impact:
Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 2.6 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |

|  |  |
|---|---|
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command '/bin/dpkg -s nis 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'nis' is not installed and no information is available
```

## 2.2.2 Ensure rsh client is not installed

### Info

The rsh-client package contains the client commands for the rsh services.
These legacy clients contain numerous security exposures and have been replaced with the more secure SSH package. Even if the server is removed, it is best to ensure the clients are also removed to prevent users from inadvertently attempting to use these commands and therefore exposing their credentials. Note that removing the rsh-client package removes the clients for rsh rcp and rlogin

### Solution

Uninstall rsh :
# apt purge rsh-client
Impact:
Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |

| | |
|---|---|
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command '/bin/dpkg -s rsh-client 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'rsh-client' is not installed and no information is available
```

## 2.2.3 Ensure talk client is not installed

### Info

The talk software makes it possible for users to send and receive messages across systems through a terminal session. The talk client, which allows initialization of talk sessions, is installed by default.
The software presents a security risk as it uses unencrypted protocols for communication.

### Solution

Uninstall talk :
# apt purge talk
Impact:
Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |

| | |
|---|---|
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

### Assets

**linux_project**

```
The command '/bin/dpkg -s talk 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'talk' is not installed and no information is available
```

## 2.2.5 Ensure ldap client is not installed

### Info

The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service that provides a method for looking up information from a central database.
If the system will not need to act as an LDAP client, it is recommended that the software be removed to reduce the potential attack surface.

### Solution

Uninstall ldap-utils :
# apt purge ldap-utils
Impact:
Removing the LDAP client will prevent or inhibit using LDAP for authentication in your environment.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |

|  |  |
|---|---|
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command '/bin/dpkg -s ldap-utils 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'ldap-utils' is not installed and no information is available
```

## 2.3.1.1 Ensure a single time synchronization daemon is in use

### Info

System time should be synchronized between all systems in an environment. This is typically done by establishing an authoritative time server or set of servers and having all systems synchronize their clocks to them.
Note:
- On virtual systems where host based time synchronization is available consult your virtualization software documentation and verify that host based synchronization is in use and follows local site policy. In this scenario, this section should be skipped
- Only one time synchronization method should be in use on the system. Configuring multiple time synchronization methods could lead to unexpected or unreliable results
Time synchronization is important to support time sensitive security mechanisms and ensures log files have consistent time records across the enterprise, which aids in forensic investigations.

### Solution

On physical systems, and virtual systems where host based time synchronization is not available.
Select one of the two time synchronization daemons; chrony (1) or systemd-timesyncd (2) and following the remediation procedure for the selected daemon.
Note: enabling more than one synchronization daemon could lead to unexpected or unreliable results:
- chrony
Run the following command to install chrony :
# apt install chrony
Run the following commands to stop and mask the systemd-timesyncd daemon:
# systemctl stop systemd-timesyncd.service
# systemctl mask systemd-timesyncd.service
Note:
- Subsection:
Configure chrony
should be followed
- Subsection:
Configure systemd-timesyncd
should be skipped
<xhtml:ol start="2"> - systemd-timesyncd
Run the following command to remove the chrony package:
# apt purge chrony # apt autoremove chrony
Note:
- Subsection:
Configure systemd-timesyncd
should be followed
- Subsection:
Configure chrony
should be skipped

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.6 |
| **800-171** | 3.3.7 |
| **800-171R3** | 03.03.06a. |
| **800-171R3** | 03.03.07 |
| **800-53** | AU-7 |
| **800-53** | AU-8 |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-8 |
| **CN-L3** | 7.1.2.3(c) |

| | |
|---|---|
| **CN-L3** | 8.1.4.3(b) |
| **CSCV7** | 6.1 |
| **CSCV8** | 8.4 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.8.17 |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-8 |
| **LEVEL** | 1A |
| **NESA** | T3.6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |
| **TBA-FIISB** | 37.4 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **
 - Only one time sync daemon is in use on the system
  - Daemon: "systemd-timesyncd.service" is enabled on the system
  - Daemon: "systemd-timesyncd.service" is active on the system
  - Daemon: "chrony.service" is not enabled and not active on the system
```

## 2.3.2.2 Ensure systemd-timesyncd is enabled and running

### Info

systemd-timesyncd is a daemon that has been added for synchronizing the system clock across the network
systemd-timesyncd needs to be enabled and running in order to synchronize the system to a timeserver.
Time synchronization is important to support time sensitive security mechanisms and to ensure log files have consistent time records across the enterprise to aid in forensic investigations

### Solution

- IF - systemd-timesyncd is in use on the system, run the following commands:
Run the following command to unmask systemd-timesyncd.service :
# systemctl unmask systemd-timesyncd.service
Run the following command to enable and start systemd-timesyncd.service :
# systemctl --now enable systemd-timesyncd.service
- OR -
If another time synchronization service is in use on the system, run the following command to stop and mask systemd-timesyncd :
# systemctl --now mask systemd-timesyncd.service

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.6 |
| **800-171** | 3.3.7 |
| **800-171R3** | 03.03.06a. |
| **800-171R3** | 03.03.07 |
| **800-53** | AU-7 |
| **800-53** | AU-8 |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-8 |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 8.1.4.3(b) |
| **CSCV7** | 6.1 |
| **CSCV8** | 8.4 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |

|  |  |
|---|---|
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.8.17 |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-8 |
| **LEVEL** | 1A |
| **NESA** | T3.6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |
| **TBA-FIISB** | 37.4 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - check if systemd-timesyncd is active
The command '/bin/systemctl is-active systemd-timesyncd.service' returned :

active

-------------------------
PASSED - systemctl is-enabled systemd-timesyncd.service
The command '/bin/systemctl is-enabled systemd-timesyncd.service' returned :

enabled
```

## 2.3.3.1 Ensure chrony is configured with authorized timeserver

### Info

-
server
- The server directive specifies an NTP server which can be used as a time source. The client-server relationship is strictly hierarchical: a client might synchronize its system time to that of the server, but the server's system time will never be influenced by that of a client.
- This directive can be used multiple times to specify multiple servers.
- The directive is immediately followed by either the name of the server, or its IP address.
-
pool
- The syntax of this directive is similar to that for the server directive, except that it is used to specify a pool of NTP servers rather than a single NTP server. The pool name is expected to resolve to multiple addresses which might change over time.
- This directive can be used multiple times to specify multiple pools.
- All options valid in the server directive can be used in this directive too.
Time synchronization is important to support time sensitive security mechanisms and to ensure log files have consistent time records across the enterprise to aid in forensic investigations

### Solution

Edit /etc/chrony/chrony.conf or a file ending insources in /etc/chrony/sources.d/ and add or edit server or pool lines as appropriate according to local site policy:
Edit the Chrony configuration and add or edit the server and/or pool lines returned by the Audit Procedure as appropriate according to local site policy
<[server|pool]> <[remote-server|remote-pool]>
Example script to add a drop-in configuration for the pool directive:
#!/usr/bin/env bash
{ [ ! -d "/etc/chrony/sources.d/" ] && mkdir /etc/chrony/sources.d/ printf '%s ' "" "#The maxsources option is unique to the pool directive" "pool time.nist.gov iburst maxsources 4" >> /etc/chrony/sources.d/60-sources.sources chronyc reload sources &>/dev/null }
Example script to add a drop-in configuration for the server directive:
#!/usr/bin/env bash
{ [ ! -d "/etc/chrony/sources.d/" ] && mkdir /etc/chrony/sources.d/ printf '%s ' "" "server time-a-g.nist.gov iburst" "server 132.163.97.3 iburst" "server time-d-b.nist.gov iburst" >> /etc/chrony/sources.d/60-sources.sources chronyc reload sources &>/dev/null }
Run the following command to reload the chronyd config:
# systemctl reload-or-restart chronyd

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.6 |
| **800-171** | 3.3.7 |
| **800-171R3** | 03.03.06a. |
| **800-171R3** | 03.03.07 |
| **800-53** | AU-7 |
| **800-53** | AU-8 |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-8 |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 8.1.4.3(b) |
| **CSCV7** | 6.1 |

|  |  |
|---|---|
| **CSCV8** | 8.4 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.8.17 |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-8 |
| **LEVEL** | 1A |
| **NESA** | T3.6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |
| **TBA-FIISB** | 37.4 |

### Assets

**linux_project**

## 2.3.3.2 Ensure chrony is running as user _chrony

### Info

The chrony package is installed with a dedicated user account _chrony This account is granted the access required by the chronyd service
The chronyd service should run with only the required privlidges

### Solution

Add or edit the user line to /etc/chrony/chrony.conf or a file ending inconf in /etc/chrony/conf.d/ :
user _chrony
- OR -
If another time synchronization service is in use on the system, run the following command to remove chrony from the system:
# apt purge chrony # apt autoremove chrony

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.6 |
| **800-171** | 3.3.7 |
| **800-171R3** | 03.03.06a. |
| **800-171R3** | 03.03.07 |
| **800-53** | AU-7 |
| **800-53** | AU-8 |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-8 |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 8.1.4.3(b) |
| **CSCV7** | 6.1 |
| **CSCV8** | 8.4 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.8.17 |

| | |
|---|---|
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-8 |
| **LEVEL** | 1A |
| **NESA** | T3.6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |
| **TBA-FIISB** | 37.4 |

### Assets

**linux_project**

## 2.3.3.3 Ensure chrony is enabled and running

### Info

chrony is a daemon for synchronizing the system clock across the network
chrony needs to be enabled and running in order to synchronize the system to a timeserver.
Time synchronization is important to support time sensitive security mechanisms and to ensure log files have consistent time records across the enterprise to aid in forensic investigations

### Solution

- IF - chrony is in use on the system, run the following commands:
Run the following command to unmask chrony.service :
# systemctl unmask chrony.service
Run the following command to enable and start chrony.service :
# systemctl --now enable chrony.service
- OR -
If another time synchronization service is in use on the system, run the following command to remove chrony :
# apt purge chrony # apt autoremove chrony

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.6 |
| **800-171** | 3.3.7 |
| **800-171R3** | 03.03.06a. |
| **800-171R3** | 03.03.07 |
| **800-53** | AU-7 |
| **800-53** | AU-8 |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-8 |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 8.1.4.3(b) |
| **CSCV7** | 6.1 |
| **CSCV8** | 8.4 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |

| | |
|---|---|
| **ISO-27001-2022** | A.8.17 |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-8 |
| **LEVEL** | 1A |
| **NESA** | T3.6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |
| **TBA-FIISB** | 37.4 |

**Assets**

**linux_project**

## 2.4.1.1 Ensure cron daemon is enabled and active

### Info

The cron daemon is used to execute batch jobs on the system.
While there may not be user jobs that need to be run on the system, the system does have maintenance jobs that may include security monitoring that have to run, and cron is used to execute them.

### Solution

- IF - cron is installed on the system:
Run the following commands to unmask, enable, and start cron :
# systemctl unmask "$(systemctl list-unit-files | awk '$1~/^crond?.service/{print $1}')"
# systemctl --now enable "$(systemctl list-unit-files | awk '$1~/^crond?.service/{print $1}')"

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171R3** | 03.04.02a. |
| **800-53** | CM-6b. |
| **800-53R5** | CM-6b. |
| **CN-L3** | 8.1.10.6(d) |
| **CSF** | PR.IP-1 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6b. |
| **LEVEL** | 1A |
| **NESA** | T3.2.1 |
| **SWIFT-CSCV1** | 2.3 |

### Assets

#### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - enabled
The command '/bin/systemctl list-unit-files | /bin/awk '$1~/^crond?\.service/{print $2}''
 returned :

enabled

-------------------------
PASSED - active
The command '/bin/systemctl list-units | /bin/awk '$1~/^crond?\.service/{print $3}'' returned :

active
```

## 2.4.2.1 Ensure at is restricted to authorized users

### Info

at allows fairly complex time specifications, extending the POSIX.2 standard. It accepts times of the form HH:MM to run a job at a specific time of day. (If that time is already past, the next day is assumed.) You may also specify midnight, noon, or teatime (4pm) and you can have a time-of-day suffixed with AM or PM for running in the morning or the evening. You can also say what day the job will be run, by giving a date in the form month-name day with an optional year, or giving a date of the form MMDD[CC]YY, MM/DD/[CC]YY, DD.MM.[CC]YY or [CC]YY-MM-DD. The specification of a date must follow the specification of the time of day. You can also give times like now + count time-units, where the time-units can be minutes, hours, days, or weeks and you can tell at to run the job today by suffixing the time with today and to run the job tomorrow by suffixing the time with tomorrow.

The /etc/at.allow and /etc/at.deny files determine which user can submit commands for later execution via at or batch. The format of the files is a list of usernames, one on each line. Whitespace is not permitted. If the file /etc/at.allow exists, only usernames mentioned in it are allowed to use at. If /etc/at.allow does not exist, /etc/at.deny is checked, every username not mentioned in it is then allowed to use at. An empty /etc/at.deny means that every user may use at. If neither file exists, only the superuser is allowed to use at.

On many systems, only the system administrator is authorized to schedule at jobs. Using the at.allow file to control who can run at jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

### Solution

- IF - at is installed on the system:
Run the following script to:
- /etc/at.allow :
- Create the file if it doesn't exist
- Change owner or user root
- If group daemon exists, change to group daemon else change group to root
- Change mode to 640 or more restrictive
- - IF - /etc/at.deny exists:
- Change owner or user root
- If group daemon exists, change to group daemon else change group to root
- Change mode to 640 or more restrictive

```
#!/usr/bin/env bash
{ grep -Pq -- '^daemonb' /etc/group && l_group="daemon" || l_group="root"
[ ! -e "/etc/at.allow" ] && touch /etc/at.allow chown root:"$l_group" /etc/at.allow chmod u-x,g-wx,o-rwx /etc/at.allow [ -e
"/etc/at.deny" ] && chown root:"$l_group" /etc/at.deny [ -e "/etc/at.deny" ] && chmod u-x,g-wx,o-rwx /etc/at.deny }
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |

| | |
|---|---|
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |

| | |
|---|---|
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |

|  |  |
|---|---|
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

**Assets**

**linux_project**

## 3.1.2 Ensure wireless interfaces are disabled

### Info

Wireless networking is used when wired networks are unavailable.
-IF- wireless is not to be used, wireless devices can be disabled to reduce the potential attack surface.

### Solution

Run the following script to disable any wireless interfaces:

```
#!/usr/bin/env bash
{ module_fix() { if ! modprobe -n -v "$l_mname" | grep -P -- '^h*install /bin/(true|false)'; then echo -e " - setting module:
\"$l_mname\" to be un-loadable"
echo -e "install $l_mname /bin/false" >> /etc/modprobe.d/"$l_mname".conf fi if lsmod | grep "$l_mname" > /dev/null
2>&1; then echo -e " - unloading module \"$l_mname\""
modprobe -r "$l_mname"
fi if ! grep -Pq -- "^h*blacklisth+$l_mnameb" /etc/modprobe.d/*; then echo -e " - deny listing \"$l_mname\""
echo -e "blacklist $l_mname" >> /etc/modprobe.d/"$l_mname".conf fi } if [ -n "$(find /sys/class/net/*/ -type d -name
wireless)" ]; then l_dname=$(for driverdir in $(find /sys/class/net/*/ -type d -name wireless | xargs -0 dirname); do
basename "$(readlink -f "$driverdir"/device/driver/module)";done | sort -u) for l_mname in $l_dname; do module_fix
done fi }
```

Impact:
Many if not all laptop workstations and some desktop workstations will connect via wireless requiring these interfaces be enabled.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 15.4 |
| **CSCV7** | 15.5 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |

|  |  |
|---|---|
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

### Assets

#### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **

 - System has no wireless NICs installed
```

## 3.1.3 Ensure bluetooth services are not in use

### Info

Bluetooth is a short-range wireless technology standard that is used for exchanging data between devices over short distances. It employs UHF radio waves in the ISM bands, from 2.402 GHz to 2.48 GHz. It is mainly used as an alternative to wire connections.
An attacker may be able to find a way to access or corrupt your data. One example of this type of activity is bluesnarfing which refers to attackers using a Bluetooth connection to steal information off of your Bluetooth device. Also, viruses or other malicious code can take advantage of Bluetooth technology to infect other devices. If you are infected, your data may be corrupted, compromised, stolen, or lost.

### Solution

Run the following commands to stop bluetooth.service and remove the bluez package:
# systemctl stop bluetooth.service # apt purge bluez
- OR -
- IF - the bluez package is required as a dependency:
Run the following commands to stop and mask bluetooth.service :
# systemctl stop bluetooth.service # systemctl mask bluetooth.service
Note: A reboot may be required
Impact:
Many personal electronic devices (PEDs) use Bluetooth technology. For example, you may be able to operate your computer with a wireless keyboard. Disabling Bluetooth will prevent these devices from connecting to the system.
There may be packages that are dependent on the bluez package. If the bluez package is removed, these dependent packages will be removed as well. Before removing the bluez package, review any dependent packages to determine if they are required on the system.
-IF- a dependent package is required: stop and mask bluetooth.service leaving the bluez package installed.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |

| | |
|---|---|
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command '/bin/dpkg -s bluez 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

dpkg-query: package 'bluez' is not installed and no information is available
```

## 3.3.3 Ensure bogus icmp responses are ignored

### Info

Setting net.ipv4.icmp_ignore_bogus_error_responses to 1 prevents the kernel from logging bogus responses (RFC-1122 non-compliant) from broadcast reframes, keeping file systems from filling up with useless log messages. Some routers (and some attackers) will send responses that violate RFC-1122 and attempt to fill up a log file system with many useless error messages.

### Solution

Set the following parameter in /etc/sysctl.conf or a file in /etc/sysctl.d/ ending inconf :
- net.ipv4.icmp_ignore_bogus_error_responses = 1

Example:

```
# printf '%s ' "net.ipv4.icmp_ignore_bogus_error_responses = 1" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

```
#!/usr/bin/env bash
{ sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1 sysctl -w net.ipv4.route.flush=1 }
```

Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |

| | |
|---|---|
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **
 - "net.ipv4.icmp_ignore_bogus_error_responses" is correctly set to "1"
    in the running configuration
 - "net.ipv4.icmp_ignore_bogus_error_responses" is correctly set to "1"
    in "/etc/ufw/sysctl.conf"
```

## 3.3.4 Ensure broadcast icmp requests are ignored

### Info

Setting net.ipv4.icmp_echo_ignore_broadcasts to 1 will cause the system to ignore all ICMP echo and timestamp requests to broadcast and multicast addresses.
Accepting ICMP echo and timestamp requests with broadcast or multicast destinations for your network could be used to trick your host into starting (or participating) in a Smurf attack. A Smurf attack relies on an attacker sending large amounts of ICMP broadcast messages with a spoofed source address. All hosts receiving this message and responding would send echo-reply messages back to the spoofed address, which is probably not routable. If many hosts respond to the packets, the amount of traffic on the network could be significantly multiplied.

### Solution

Set the following parameter in /etc/sysctl.conf or a file in /etc/sysctl.d/ ending inconf :
- net.ipv4.icmp_echo_ignore_broadcasts = 1
Example:

```
# printf '%s ' "net.ipv4.icmp_echo_ignore_broadcasts = 1" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following script to set the active kernel parameters:

```
#!/usr/bin/env bash
{ sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1 sysctl -w net.ipv4.route.flush=1 }
```

Note: If these settings appear in a canonically later file, or later in the same file, these settings will be overwritten

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |

|  |  |
|---|---|
| **ITSG-33** | CM-7 |
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **
 - "net.ipv4.icmp_echo_ignore_broadcasts" is correctly set to "1"
    in the running configuration
 - "net.ipv4.icmp_echo_ignore_broadcasts" is correctly set to "1"
    in "/etc/ufw/sysctl.conf"
```

## 4.1.1 Ensure a single firewall configuration utility is in use

### Info

In Linux security, employing a single, effective firewall configuration utility ensures that only legitimate traffic gets processed, reducing the system's exposure to potential threats. The choice between ufw nftables and iptables depends on organizational needs.
Note: iptables is being phased out, and support for iptables will be reduced over time. It is recommended to transition towards either nftables or ufw as the default firewall management tool.
Proper configuration of a single firewall utility minimizes cyber threats and protects services and data, while avoiding vulnerabilities like open ports or exposed services. Standardizing on a single tool simplifies management, reduces errors, and fortifies security across Linux systems.

### Solution

Remediating to a single firewall configuration is a complex process and involves several steps. The following provides the basic steps to follow for a single firewall configuration:
-
Determine which firewall utility best fits organizational needs
-
Follow the recommendations in the subsequent subsection for the single firewall to be used
Note: Review the firewall subsection overview for the selected firewall to be used, it contains a script tosimplify this process.
-
Return to this recommendation to ensure a single firewall configuration utility is in use
Impact:
The use of more than one firewall utility may produce unexpected results.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |

| | |
|---|---|
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |

| | |
|---|---|
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

## Assets

### linux_project

```
The command script with multiple lines returned :

Audit Results:
 ** PASS **
 - A single firewall is in use follow the recommendation in iptables subsection ONLY
```

## 4.2.1 Ensure ufw is installed

### Info

The Uncomplicated Firewall (ufw) is a frontend for iptables and is particularly well-suited for host-based firewalls. ufw provides a framework for managing netfilter, as well as a command-line interface for manipulating the firewall
A firewall utility is required to configure the Linux kernel's netfilter framework via the iptables or nftables back-end.
The Linux kernel's netfilter framework host-based firewall can protect against threats originating from within a corporate network to include malicious mobile code and poorly configured software on a host.
Note: Only one firewall utility should be installed and configured. UFW is dependent on the iptables package
NOTE: The identified firewall 'ufw' was not found to be active and this check does not apply.

### Solution

Run the following command to install Uncomplicated Firewall (UFW):
# apt install ufw

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |
| **CSF2.0** | DE.CM-01 |

| | |
|---|---|
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |

|  |  |
|---|---|
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

**Assets**

**linux_project**

## 4.2.2 Ensure iptables-persistent is not installed with ufw

### Info

The iptables-persistent is a boot-time loader for netfilter rules, iptables plugin
Running both ufw and the services included in the iptables-persistent package may lead to conflict
NOTE: The identified firewall 'ufw' was not found to be active and this check does not apply.

### Solution

Run the following command to remove the iptables-persistent package:

```
# apt purge iptables-persistent
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |

| | |
|---|---|
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |

| | |
|---|---|
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

| **Assets** |
|---|
| **linux_project** |

## 4.2.3 Ensure ufw service is enabled

### Info

UncomplicatedFirewall (ufw) is a frontend for iptables. ufw provides a framework for managing netfilter, as well as a command-line and available graphical user interface for manipulating the firewall.
Note:
- When running ufw enable or starting ufw via its initscript, ufw will flush its chains. This is required so ufw can maintain a consistent state, but it may drop existing connections (eg ssh). ufw does support adding rules before enabling the firewall.
- Run the following command before running ufw enable
# ufw allow proto tcp from any to any port 22
- The rules will still be flushed, but the ssh port will be open after enabling the firewall. Please note that once ufw is 'enabled', ufw will not flush the chains when adding or removing rules (but will when modifying a rule or changing the default policy)
- By default, ufw will prompt when enabling the firewall while running under ssh. This can be disabled by using ufw --force enable
The ufw service must be enabled and running in order for ufw to protect the system
NOTE: The identified firewall 'ufw' was not found to be active and this check does not apply.

### Solution

Run the following command to unmask the ufw daemon:
# systemctl unmask ufw.service
Run the following command to enable and start the ufw daemon:
# systemctl --now enable ufw.service
active
Run the following command to enable ufw:
# ufw enable
Impact:
Changing firewall settings while connected over network can result in being locked out of the system.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |

| | |
|---|---|
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |

| | |
|---|---|
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

| **Assets** |
|---|
| **linux_project** |

## 4.2.4 Ensure ufw loopback traffic is configured

### Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8 for IPv4 and ::1/128 for IPv6).
Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8 for IPv4 and ::1/128 for IPv6) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.
NOTE: The identified firewall 'ufw' was not found to be active and this check does not apply.

### Solution

Run the following commands to configure the loopback interface to accept traffic:
# ufw allow in on lo # ufw allow out on lo
Run the following commands to configure all other interfaces to deny traffic to the loopback network:
# ufw deny in from 127.0.0.0/8 # ufw deny in from ::1

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |

| | |
|---|---|
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |

| | |
|---|---|
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

**Assets**

**linux_project**

## 4.2.5 Ensure ufw outbound connections are configured

### Info

Configure the firewall rules for new outbound connections.
Note:
- Changing firewall settings while connected over network can result in being locked out of the system.
- Unlike iptables, when a new outbound rule is added, ufw automatically takes care of associated established connections, so no rules for the latter kind are required.
If rules are not in place for new outbound connections all packets will be dropped by the default policy preventing network usage.
NOTE: The identified firewall 'ufw' was not found to be active and this check does not apply.

### Solution

Configure ufw in accordance with site policy. The following commands will implement a policy to allow all outbound connections on all interfaces:
# ufw allow out on all

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |

| | |
|---|---|
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1M |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |

| | |
|---|---|
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

**Assets**

**linux_project**

## 4.2.6 Ensure ufw firewall rules exist for all open ports

### Info

Services and ports can be accepted or explicitly rejected.
Note:
- Changing firewall settings while connected over network can result in being locked out of the system
- The remediation command opens up the port to traffic from all sources. Consult ufw documentation and set any restrictions in compliance with site policy
To reduce the attack surface of a system, all services and ports should be blocked unless required.
- Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.
- Without a firewall rule configured for open ports, the default firewall policy will drop all packets to these ports.
- Required ports should have a firewall rule created to allow approved connections in accordance with local site policy.
- Unapproved ports should have an explicit deny rule created.
NOTE: The identified firewall 'ufw' was not found to be active and this check does not apply.

### Solution

For each port identified in the audit which does not have a firewall rule, evaluate the service listening on the port and add a rule for accepting or denying inbound connections in accordance with local site policy:
Examples:
# ufw allow in <port>/<tcp or udp protocol>
# ufw deny in <port>/<tcp or udp protocol>
Note: Examples create rules for from any, to any. More specific rules should be concentered when allowing inbound traffic e.g only traffic from this network.
Example to allow traffic on port 443 using the tcp protocol from the 192.168.1.0 network:
ufw allow from 192.168.1.0/24 to any proto tcp port 443

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |

| | |
|---|---|
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |

| | |
|---|---|
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

**Assets**

**linux_project**

## 4.2.7 Ensure ufw default deny firewall policy

### Info

A default deny policy on connections ensures that any unconfigured network usage will be rejected.
Note: Any port or protocol without a explicit allow before the default deny will be blocked
With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to allow list acceptable usage than to deny list unacceptable usage.
NOTE: The identified firewall 'ufw' was not found to be active and this check does not apply.

### Solution

Run the following commands to implement a default
deny
policy:
# ufw default deny incoming # ufw default deny outgoing # ufw default deny routed
Impact:
Any port and protocol not explicitly allowed will be blocked. The following rules should be considered before applying the default deny.
ufw allow out http ufw allow out https ufw allow out ntp # Network Time Protocol ufw allow out to any port 53 # DNS ufw allow out to any port 853 # DNS over TLS ufw logging on

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |

| | |
|---|---|
| **CSF** | PR.PT-4 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |

| | |
|---|---|
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

**Assets**

**linux_project**

## 4.3.1 Ensure nftables is installed

### Info

nftables provides a new in-kernel packet classification framework that is based on a network-specific Virtual Machine (VM) and a new nft userspace command line tool. nftables reuses the existing Netfilter subsystems such as the existing hook infrastructure, the connection tracking system, NAT, userspace queuing and logging subsystem.
Notes:
- nftables is available in Linux kernel 3.13 and newer
- Only one firewall utility should be installed and configured
- Changing firewall settings while connected over the network can result in being locked out of the system
nftables is a subsystem of the Linux kernel that can protect against threats originating from within a corporate network to include malicious mobile code and poorly configured software on a host.
NOTE: The identified firewall 'nftables' was not found to be active and this check does not apply.

### Solution

Run the following command to install nftables :
# apt install nftables

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |

| | |
|---|---|
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |

|  |  |
|---|---|
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

**Assets**

**linux_project**

## 4.3.10 Ensure nftables rules are permanent

### Info

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames.
The nftables service reads the /etc/nftables.conf file for a nftables file or files to include in the nftables ruleset.
A nftables ruleset containing the input, forward, and output base chains allow network traffic to be filtered.
Note: Saving the script and following the instruction in the Configure nftables section overview will implement the rules in the configure nftable section, open port 22(ssh) from anywhere, and applies nftables ruleset on boot.
Changes made to nftables ruleset only affect the live system, you will also need to configure the nftables ruleset to apply on boot
NOTE: The identified firewall 'nftables' was not found to be active and this check does not apply.

### Solution

Edit the /etc/nftables.conf file and un-comment or add a line with include <Absolute path to nftables rules file> for each nftables file you want included in the nftables ruleset on boot
Example:

```
# vi /etc/nftables.conf
```

Add the line:

```
include "/etc/nftables.rules"
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |

| | |
|---|---|
| **CSF** | PR.PT-4 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |

| | |
|---|---|
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

**Assets**

**linux_project**

## 4.3.2 Ensure ufw is uninstalled or disabled with nftables

### Info

Uncomplicated Firewall (UFW) is a program for managing a netfilter firewall designed to be easy to use.
Running both the nftables service and ufw may lead to conflict and unexpected results.
NOTE: The identified firewall 'nftables' was not found to be active and this check does not apply.

### Solution

Run one of the following to either remove ufw or disable ufw and mask ufw.service :
Run the following command to remove ufw :
# apt purge ufw
-OR-
Run the following commands to disable ufw and mask ufw.service :
# ufw disable # systemctl stop ufw.service # systemctl mask ufw.service
Note: ufw disable needs to be run before systemctl mask ufw.service in order to correctly disable UFW

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |

| | |
|---|---|
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |

| | |
|---|---|
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

**Assets**

**linux_project**

## 4.3.3 Ensure iptables are flushed with nftables

### Info

nftables is a replacement for iptables, ip6tables, ebtables and arptables
It is possible to mix iptables and nftables. However, this increases complexity and also the chance to introduce errors.
For simplicity flush out all iptables rules, and ensure it is not loaded
NOTE: The identified firewall 'nftables' was not found to be active and this check does not apply.

### Solution

Run the following commands to flush iptables:
For iptables:

```
# iptables -F
```

For ip6tables:

```
# ip6tables -F
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |
| **CSF2.0** | DE.CM-01 |

| | |
|---|---|
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1M |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |

| | |
|---|---|
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

**Assets**

**linux_project**

## 4.3.4 Ensure a nftables table exists

### Info

Tables hold chains. Each table only has one address family and only applies to packets of this family. Tables can have one of five families.

nftables doesn't have any default tables. Without a table being built, nftables will not filter network traffic.

NOTE: The identified firewall 'nftables' was not found to be active and this check does not apply.

### Solution

Run the following command to create a table in nftables

```
# nft create table inet <table name>
```

Example:

```
# nft create table inet filter
```

Impact:

Adding rules to a running nftables can cause loss of connectivity to the system

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |

| | |
|---|---|
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |

| | |
|---|---|
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

**Assets**

**linux_project**

## 4.3.5 Ensure nftables base chains exist

### Info

Chains are containers for rules. They exist in two kinds, base chains and regular chains. A base chain is an entry point for packets from the networking stack, a regular chain may be used as jump target and is used for better rule organization.
If a base chain doesn't exist with a hook for input, forward, and delete, packets that would flow through those chains will not be touched by nftables.
NOTE: The identified firewall 'nftables' was not found to be active and this check does not apply.

### Solution

Run the following command to create the base chains:

```
# nft create chain inet <table name> <base chain name> { type filter hook <(input|forward|output)> priority 0 ; }
```

Example:

```
# nft create chain inet filter input { type filter hook input priority 0 ; }
# nft create chain inet filter forward { type filter hook forward priority 0 ; }
# nft create chain inet filter output { type filter hook output priority 0 ; }
```

Impact:
If configuring nftables over ssh, creating a base chain with a policy of drop will cause loss of connectivity.
Ensure that a rule allowing ssh has been added to the base chain prior to setting the base chain's policy to drop

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |

| | |
|---|---|
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |

| | |
|---|---|
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

**Assets**

**linux_project**

## 4.3.6 Ensure nftables loopback traffic is configured

### Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network
Loopback traffic is generated between processes on machine and is typically critical to the operation of the system.
The loopback interface is the only place that loopback network traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.
NOTE: The identified firewall 'nftables' was not found to be active and this check does not apply.

### Solution

Run the following commands to implement the loopback rules:
# nft add rule inet filter input iif lo accept # nft add rule inet filter input ip saddr 127.0.0.0/8 counter drop
- IF - IPv6 is enabled on the system:
Run the following command to implement the IPv6 loopback rule:
# nft add rule inet filter input ip6 saddr ::1 counter drop

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |

| | |
|---|---|
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |

| | |
|---|---|
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

| Assets |
|---|
| **linux_project** |

## 4.3.7 Ensure nftables outbound and established connections are configured

### Info

Configure the firewall rules for new outbound, and established connections
If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.
NOTE: The identified firewall 'nftables' was not found to be active and this check does not apply.

### Solution

Configure nftables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

```
# nft add rule inet filter input ip protocol tcp ct state established accept
# nft add rule inet filter input ip protocol udp ct state established accept
# nft add rule inet filter output ip protocol tcp ct state new,related,established accept
# nft add rule inet filter output ip protocol udp ct state new,related,established accept
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |

| | |
|---|---|
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1M |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |

| | |
|---|---|
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

**Assets**

**linux_project**

## 4.3.8 Ensure nftables default deny firewall policy

### Info

Base chain policy is the default verdict that will be applied to packets reaching the end of the chain.
There are two policies: accept (Default) and drop. If the policy is set to accept the firewall will accept any packet that is not configured to be denied and the packet will continue transversing the network stack.
It is easier to allow list acceptable usage than to deny list unacceptable usage.
Note:
- Allow port 22(ssh) needs to be updated to only allow systems requiring ssh connectivity to connect, as per site policy.
- Changing firewall settings while connected over network can result in being locked out of the system.
NOTE: The identified firewall 'nftables' was not found to be active and this check does not apply.

### Solution

Run the following command for the base chains with the input, forward, and output hooks to implement a default DROP policy:
# nft chain <table family> <table name> <chain name> { policy drop ; }
Example:
# nft chain inet filter input { policy drop ; }
# nft chain inet filter forward { policy drop ; }
# nft chain inet filter output { policy drop ; }
Impact:
If configuring nftables over ssh, creating a base chain with a policy of drop will cause loss of connectivity.
Ensure that a rule allowing ssh has been added to the base chain prior to setting the base chain's policy to drop

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |

| | |
|---|---|
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |

| | |
|---|---|
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

**Assets**

**linux_project**

## 4.3.9 Ensure nftables service is enabled

### Info

The nftables service allows for the loading of nftables rulesets during boot, or starting on the nftables service
The nftables service restores the nftables rules from the rules files referenced in the /etc/nftables.conf file during boot or the starting of the nftables service
NOTE: The identified firewall 'nftables' was not found to be active and this check does not apply.

### Solution

Run the following command to enable the nftables service:
# systemctl enable nftables

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |

| | |
|---|---|
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |

|  |  |
|---|---|
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

**Assets**

**linux_project**

## 4.4.1.1 Ensure iptables packages are installed

### Info

iptables is a utility program that allows a system administrator to configure the tables provided by the Linux kernel firewall, implemented as different Netfilter modules, and the chains and rules it stores. Different kernel modules and programs are used for different protocols; iptables applies to IPv4, ip6tables to IPv6, arptables to ARP, and ebtables to Ethernet frames.
A method of configuring and maintaining firewall rules is necessary to configure a Host Based Firewall.

### Solution

Run the following command to install iptables and iptables-persistent
# apt install iptables iptables-persistent

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |

| | |
|---|---|
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |

| | |
|---|---|
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - dpkg check iptables-persistent
The command '/bin/dpkg -s iptables-persistent 2>&1 | /bin/grep -E '(Status:|not installed)''
 returned :

Status: install ok installed

-------------------------
PASSED - dpkg check iptables
The command '/bin/dpkg -s iptables 2>&1 | /bin/grep -E '(Status:|not installed)'' returned :

Status: install ok installed
```

## 4.4.1.2 Ensure nftables is not in use with iptables

### Info

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames and is the successor to iptables.
Running both iptables and nftables may lead to conflict.

### Solution

Run the following command to remove nftables :
# apt purge nftables
- OR -
Run the following commands to stop and mask nftables.service :
# systemctl stop nftables.service # systemctl mask nftables.service

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |
| **CSF2.0** | DE.CM-01 |

| | |
|---|---|
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |

|  |  |
|---|---|
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - ensure nftables disabled
The command '/bin/systemctl is-enabled nftables.service 2>/dev/null | /bin/grep '^enabled' | /bin/
awk '{print} END {if(NR==0) print "disabled" }'' returned :

disabled

-------------------------
PASSED - ensure nftables inactive
The command '/bin/systemctl is-active nftables.service 2>/dev/null | /bin/grep '^active' | /bin/
awk '{print} END {if(NR==0) print "inactive" }'' returned :

inactive
```

## 4.4.1.3 Ensure ufw is not in use with iptables

### Info

Uncomplicated Firewall (UFW) is a program for managing a netfilter firewall designed to be easy to use.
- Uses a command-line interface consisting of a small number of simple commands
- Uses iptables for configuration
Running iptables.persistent with ufw enabled may lead to conflict and unexpected results.

### Solution

Run the following command to remove ufw :
# apt purge ufw
- OR -
Run the following commands to disable ufw, and stop and mask ufw.service :
# ufw disable # systemctl stop ufw.service # systemctl mask ufw.service
Note: ufw disable needs to be run before systemctl mask ufw.service in order to correctly disable UFW

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |

| | |
|---|---|
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |

|  |  |
|---|---|
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

## Assets

### linux_project

```
The command '/bin/dpkg -s ufw 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

Status: deinstall ok config-files
```

## 5.1.10 Ensure sshd HostbasedAuthentication is disabled

### Info

The HostbasedAuthentication parameter specifies if authentication is allowed through trusted hosts via the user ofrhosts or /etc/hosts.equiv along with successful public key client host authentication.
Even though therhosts files are ineffective if support is disabled in /etc/pam.conf disabling the ability to userhosts files in SSH provides an additional layer of protection.

### Solution

Edit the /etc/ssh/sshd_config file to set the HostbasedAuthentication parameter to no above any Include and Match entries as follows:
HostbasedAuthentication no
Note: First occurrence of a option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.06b. |
| **800-53** | CM-7b. |
| **800-53R5** | CM-7b. |
| **CN-L3** | 7.1.3.5(c) |
| **CN-L3** | 7.1.3.7(d) |
| **CN-L3** | 8.1.4.4(b) |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ITSG-33** | CM-7a. |
| **LEVEL** | 1A |
| **NIAV2** | SS13b |
| **NIAV2** | SS14a |
| **NIAV2** | SS14c |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **PCI-DSSV4.0** | 2.2.4 |
| **QCSC-V1** | 3.2 |

| | |
|---|---|
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

port 22: hostbasedauthentication no
Pass
```

## 5.1.11 Ensure sshd IgnoreRhosts is enabled

### Info

The IgnoreRhosts parameter specifies thatrhosts andshosts files will not be used in RhostsRSAAuthentication or HostbasedAuthentication
Setting this parameter forces users to enter a password when authenticating with SSH.

### Solution

Edit the /etc/ssh/sshd_config file to set the IgnoreRhosts parameter to yes above any Include and Match entries as follows:
IgnoreRhosts yes
Note: First occurrence of a option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

### Assets

**linux_project**

```
The command script with multiple lines returned :

port 22: ignorerhosts yes
Pass
```

## 5.1.12 Ensure sshd KexAlgorithms is configured

### Info

Key exchange is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received

Notes:

- Kex algorithms have a higher preference the earlier they appear in the list
- Some organizations may have stricter requirements for approved Key exchange algorithms
- Ensure that Key exchange algorithms used are in compliance with site policy
- The only Key Exchange Algorithms currently FIPS 140 approved are:
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- diffie-hellman-group-exchange-sha256
- diffie-hellman-group16-sha512
- diffie-hellman-group18-sha512
- diffie-hellman-group14-sha256

Key exchange methods that are considered weak should be removed. A key exchange method may be weak because too few bits are used, or the hashing algorithm is considered too weak. Using weak algorithms could expose connections to man-in-the-middle attacks

### Solution

Edit the /etc/ssh/sshd_config file and add/modify the KexAlgorithms line to contain a comma separated list of the site unapproved (weak) KexAlgorithms preceded with a - above any Include entries:

Example:

KexAlgorithms -diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1

Note: First occurrence of an option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.13 |
| **800-171** | 3.5.2 |
| **800-171** | 3.13.8 |
| **800-171R3** | 03.05.07 |
| **800-171R3** | 03.05.12 |
| **800-171R3** | 03.13.08 |
| **800-53** | AC-17(2) |
| **800-53** | IA-5 |
| **800-53** | IA-5(1) |
| **800-53** | SC-8 |
| **800-53** | SC-8(1) |
| **800-53R5** | AC-17(2) |
| **800-53R5** | IA-5 |
| **800-53R5** | IA-5(1) |
| **800-53R5** | SC-8 |

| | |
|---|---|
| **800-53R5** | SC-8(1) |
| **CN-L3** | 7.1.2.7(g) |
| **CN-L3** | 7.1.3.1(d) |
| **CN-L3** | 8.1.2.2(a) |
| **CN-L3** | 8.1.2.2(b) |
| **CN-L3** | 8.1.4.1(c) |
| **CN-L3** | 8.1.4.7(a) |
| **CN-L3** | 8.1.4.8(a) |
| **CN-L3** | 8.2.4.5(c) |
| **CN-L3** | 8.2.4.5(d) |
| **CN-L3** | 8.5.2.2 |
| **CSCV7** | 14.4 |
| **CSCV8** | 3.10 |
| **CSF** | PR.AC-1 |
| **CSF** | PR.AC-3 |
| **CSF** | PR.DS-2 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-02 |
| **GDPR** | 32.1.a |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **HIPAA** | 164.312(e)(1) |
| **HIPAA** | 164.312(e)(2)(i) |
| **ISO-27001-2022** | A.5.10 |

| | |
|---|---|
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.6.7 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.2.2 |
| **ISO/IEC-27001** | A.10.1.1 |
| **ISO/IEC-27001** | A.13.2.3 |
| **ITSG-33** | AC-17(2) |
| **ITSG-33** | IA-5 |
| **ITSG-33** | IA-5(1) |
| **ITSG-33** | SC-8 |
| **ITSG-33** | SC-8a. |
| **ITSG-33** | SC-8(1) |
| **LEVEL** | 1A |
| **NESA** | T4.3.1 |
| **NESA** | T4.3.2 |
| **NESA** | T4.5.1 |
| **NESA** | T4.5.2 |
| **NESA** | T5.2.3 |
| **NESA** | T5.4.2 |
| **NESA** | T7.3.3 |
| **NESA** | T7.4.1 |
| **NIAV2** | AM37 |
| **NIAV2** | IE8 |
| **NIAV2** | IE9 |
| **NIAV2** | IE12 |
| **NIAV2** | NS5d |
| **NIAV2** | NS6b |
| **NIAV2** | NS29 |

| | |
|---|---|
| **NIAV2** | SS24 |
| **PCI-DSSV3.2.1** | 2.3 |
| **PCI-DSSV3.2.1** | 4.1 |
| **PCI-DSSV4.0** | 2.2.7 |
| **PCI-DSSV4.0** | 4.2.1 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 2.1 |
| **SWIFT-CSCV1** | 2.6 |
| **SWIFT-CSCV1** | 4.1 |
| **TBA-FIISB** | 29.1 |

## Assets

### linux_project

```
The command script with multiple lines returned :

port 22: kexalgorithms sntrup761x25519-sha512@openssh.com,curve25519-sha256,curve25519-
sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-
exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-
group14-sha256
Pass
```

## 5.1.14 Ensure sshd LogLevel is configured

### Info

SSH provides several logging levels with varying amounts of verbosity. The DEBUG options are specifically not recommended other than strictly for debugging SSH communications. These levels provide so much data that it is difficult to identify important security information, and may violate the privacy of users.
The INFO level is the basic level that only records login activity of SSH users. In many situations, such as Incident Response, it is important to determine when a particular user was active on a system. The logout record can eliminate those users who disconnected, which helps narrow the field.
The VERBOSE level specifies that login and logout activity as well as the key fingerprint for any SSH key used for login will be logged. This information is important for SSH key management, especially in legacy environments.

### Solution

Edit the /etc/ssh/sshd_config file to set the LogLevel parameter to VERBOSE or INFO above any Include and Match entries as follows:
LogLevel VERBOSE
- OR - LogLevel INFO
Note: First occurrence of an option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171** | 3.3.6 |
| **800-171R3** | 03.03.01 |
| **800-171R3** | 03.03.03 |
| **800-171R3** | 03.03.06a. |
| **800-53** | AU-2 |
| **800-53** | AU-7 |
| **800-53** | AU-12 |
| **800-53R5** | AU-2 |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-12 |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 8.1.4.3(a) |
| **CSCV7** | 6.2 |
| **CSCV7** | 6.3 |
| **CSCV8** | 8.2 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |

| | |
|---|---|
| **CSF** | DE.CM-7 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.8.15 |
| **ITSG-33** | AU-2 |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-12 |
| **LEVEL** | 1A |
| **NESA** | M1.2.2 |
| **NESA** | M5.5.1 |
| **NIAV2** | AM7 |
| **NIAV2** | AM11a |
| **NIAV2** | AM11b |
| **NIAV2** | AM11c |
| **NIAV2** | AM11d |
| **NIAV2** | AM11e |
| **NIAV2** | SS30 |
| **NIAV2** | VL8 |
| **PCI-DSSV3.2.1** | 10.1 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 6.2 |

| | |
|---|---|
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |

## Assets

### linux_project

```
The command script with multiple lines returned :

port 22: loglevel INFO
Pass
```

## 5.1.17 Ensure sshd MaxSessions is configured

### Info

The MaxSessions parameter specifies the maximum number of open sessions permitted from a given connection.
To protect a system from denial of service due to a large number of concurrent sessions, use the rate limiting function of MaxSessions to protect availability of sshd logins and prevent overwhelming the daemon.

### Solution

Edit the /etc/ssh/sshd_config file to set the MaxSessions parameter to 10 or less above any Include and Match entries as follows:
MaxSessions 10
Note: First occurrence of an option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-53** | AC-10 |
| **800-53R5** | AC-10 |
| **CSF2.0** | PR.AA-05 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ITSG-33** | AC-10 |
| **LEVEL** | 1A |
| **NESA** | T5.5.1 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |

### Assets

#### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - config file MaxSessions setting
The following file(s) do not contain "^[\s]*(?i)MaxSessions(?-i)[\s]":
      /etc/ssh/sshd_config
      /etc/ssh/sshd_config.d/50-cloud-init.conf
      /etc/ssh/sshd_config.d/60-cloudimg-settings.conf

-------------------------
PASSED - sshd maxsessions setting
The command script with multiple lines returned :

port 22: maxsessions 10
Pass
```

## 5.1.19 Ensure sshd PermitEmptyPasswords is disabled

### Info

The PermitEmptyPasswords parameter specifies if the SSH server allows login to accounts with empty password strings.
Disallowing remote shell access to accounts that have an empty password reduces the probability of unauthorized access to the system.

### Solution

Edit /etc/ssh/sshd_config and set the PermitEmptyPasswords parameter to no above any Include and Match entries as follows:
PermitEmptyPasswords no
Note: First occurrence of an option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

### Assets

### linux_project

```
The command script with multiple lines returned :

port 22: permitemptypasswords no
Pass
```

## 5.1.2 Ensure permissions on SSH private host key files are configured

### Info

An SSH private key is one of two files used in SSH public key authentication. In this authentication method, the possession of the private key is proof of identity. Only a private key that corresponds to a public key will be able to authenticate successfully. The private keys need to be stored and handled carefully, and no copies of the private key should be distributed.
If an unauthorized user obtains the private SSH host key file, the host could be impersonated

### Solution

Run the following script to set mode, ownership, and group on the private SSH host key files:

```
#!/usr/bin/env bash
{ a_output=(); a_output2=(); l_ssh_group_name="$(awk -F: '($1 ~ /^(ssh_keys|_?ssh)$/) {print $1}' /etc/group)"
f_file_access_fix() { while IFS=: read -r l_file_mode l_file_owner l_file_group; do a_out2=() [ "$l_file_group" =
"$l_ssh_group_name" ] && l_pmask="0137" || l_pmask="0177"
l_maxperm="$( printf '%o' $(( 0777 & ~$l_pmask )) )"
if [ $(( $l_file_mode & $l_pmask )) -gt 0 ]; then a_out2+=(" Mode: \"$l_file_mode\" should be mode: \"$l_maxperm\" or
more restrictive" " updating to mode: :$l_maxperm\"") if [ "l_file_group" = "$l_ssh_group_name" ]; then chmod u-x,g-
wx,o-rwx "$l_file"
else chmod u-x,go-rwx "$l_file"
fi fi if [ "$l_file_owner" != "root" ]; then a_out2+=(" Owned by: \"$l_file_owner\" should be owned by \"root\"" " Changing
ownership to \"root\"") chown root "$l_file"
fi if [[ ! "$l_file_group" =~ ($l_ssh_group_name|root) ]]; then [ -n "$l_ssh_group_name" ] &&
l_new_group="$l_ssh_group_name" || l_new_group="root"
a_out2+=(" Owned by group \"$l_file_group\" should be group owned by: \"$l_ssh_group_name\" or \"root\"" "
Changing group ownership to \"$l_new_group\"") chgrp "$l_new_group" "$l_file"
fi if [ "${#a_out2[@]}" -gt "0" ]; then a_output2+=(" - File: \"$l_file\"" "${a_out2[@]}") else a_output+=(" - File: \"$l_file
\"" "Correct: mode: \"$l_file_mode\", owner: \"$l_file_owner\", and group owner: \"$l_file_group\" configured") fi done
< <(stat -Lc '%#a:%U:%G' "$l_file") } while IFS= read -r -d $'0' l_file; do if ssh-keygen -lf &>/dev/null "$l_file"; then file
"$l_file" | grep -Piq -- 'bopensshh+([^# r]+h+)?privateh+keyb' && f_file_access_fix fi done < <(find -L /etc/ssh -xdev -
type f -print0 2>/dev/null) if [ "${#a_output2[@]}" -le "0" ]; then printf '%s ' "" " - No access changes required" ""
else printf '%s ' "" " - Remediation results:" "${a_output2[@]}" ""
fi }
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |

| | |
|---|---|
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |

| | |
|---|---|
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |

| | |
|---|---|
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **
  - File: "/etc/ssh/ssh_host_rsa_key"
    Correct: mode: "0600", owner: "root" and group owner: "root" configured
  - File: "/etc/ssh/ssh_host_ed25519_key"
    Correct: mode: "0600", owner: "root" and group owner: "root" configured
  - File: "/etc/ssh/ssh_host_ecdsa_key"
    Correct: mode: "0600", owner: "root" and group owner: "root" configured
```

## 5.1.21 Ensure sshd PermitUserEnvironment is disabled

### Info

The PermitUserEnvironment option allows users to present environment options to the SSH daemon.
Permitting users the ability to set environment variables through the SSH daemon could potentially allow users to bypass security controls (e.g. setting an execution path that has SSH executing trojan'd programs)

### Solution

Edit the /etc/ssh/sshd_config file to set the PermitUserEnvironment parameter to no above any Include entries as follows:
PermitUserEnvironment no
Note: First occurrence of an option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.06b. |
| **800-53** | CM-7b. |
| **800-53R5** | CM-7b. |
| **CN-L3** | 7.1.3.5(c) |
| **CN-L3** | 7.1.3.7(d) |
| **CN-L3** | 8.1.4.4(b) |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ITSG-33** | CM-7a. |
| **LEVEL** | 1A |
| **NIAV2** | SS13b |
| **NIAV2** | SS14a |
| **NIAV2** | SS14c |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **PCI-DSSV4.0** | 2.2.4 |
| **QCSC-V1** | 3.2 |
| **SWIFT-CSCV1** | 2.3 |

### Assets

### linux_project

```
The command script with multiple lines returned :

port 22: permituserenvironment no
Pass
```

## 5.1.22 Ensure sshd UsePAM is enabled

### Info

The UsePAM directive enables the Pluggable Authentication Module (PAM) interface. If set to yes this will enable PAM authentication using ChallengeResponseAuthentication and PasswordAuthentication directives in addition to PAM account and session module processing for all authentication types.

When usePAM is set to yes PAM runs through account and session types properly. This is important if you want to restrict access to services based off of IP, time or other factors of the account. Additionally, you can make sure users inherit certain environment variables on login or disallow access to the server

### Solution

Edit the /etc/ssh/sshd_config file to set the UsePAM parameter to yes above any Include entries as follows:

UsePAM yes

Note: First occurrence of an option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

### Assets

### linux_project

```
The command script with multiple lines returned :

port 22: usepam yes
Pass
```

## 5.1.3 Ensure permissions on SSH public host key files are configured

### Info

An SSH public key is one of two files used in SSH public key authentication. In this authentication method, a public key is a key that can be used for verifying digital signatures generated using a corresponding private key. Only a public key that corresponds to a private key will be able to authenticate successfully.
If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

### Solution

Run the following script to set mode, ownership, and group on the public SSH host key files:

```
#!/usr/bin/env bash
{ a_output=(); a_output2=() l_pmask="0133"; l_maxperm="$( printf '%o' $(( 0777 & ~$l_pmask )) )"
f_file_access_fix() { while IFS=: read -r l_file_mode l_file_owner l_file_group; do a_out2=() [ $(( $l_file_mode &
$l_pmask )) -gt 0 ] && a_out2+=(" Mode: \"$l_file_mode\" should be mode: \"$l_maxperm\" or more restrictive" "
updating to mode: \"$l_maxperm\"") && chmod u-x,go-wx "$l_file"
[ "$l_file_owner" != "root" ] && a_out2+=(" Owned by: \"$l_file_owner\" should be owned by \"root\"" " Changing
ownership to \"root\"") && chown root "$l_file"
[ "$l_file_group" != "root" ] && a_out2+=(" Owned by group \"$l_file_group\" should be group owned by: \"root\"" "
Changing group ownership to \"root\"") && chgrp root "$l_file"
if [ "${#a_out2[@]}" -gt "0" ]; then a_output2+=(" - File: \"$l_file\"" "${a_out2[@]}") else a_output+=(" - File: \"$l_file\""
" Correct: mode: \"$l_file_mode\", owner: \"$l_file_owner\", and group owner: \"$l_file_group\" configured") fi done <
<(stat -Lc '%#a:%U:%G' "$l_file") } while IFS= read -r -d $'0' l_file; do if ssh-keygen -lf &>/dev/null "$l_file"; then file
"$l_file" | grep -Piq -- 'bopensshh+([^# r]+h+)?publich+keyb' && f_file_access_fix fi done < <(find -L /etc/ssh -xdev -
type f -print0 2>/dev/null) if [ "${#a_output2[@]}" -le "0" ]; then printf '%s ' "" " - No access changes required" ""
else printf '%s ' " - Remediation results:" "${a_output2[@]}" ""
fi }
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |

| | |
|---|---|
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |

| | |
|---|---|
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |

|  |  |
|---|---|
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **
  - File: "/etc/ssh/ssh_host_ed25519_key.pub"
    Correct: mode: "0644", owner: "root" and group owner: "root" configured
  - File: "/etc/ssh/ssh_host_rsa_key.pub"
    Correct: mode: "0644", owner: "root" and group owner: "root" configured
  - File: "/etc/ssh/ssh_host_ecdsa_key.pub"
    Correct: mode: "0644", owner: "root" and group owner: "root" configured
```

## 5.2.1 Ensure sudo is installed

### Info

sudo allows a permitted user to execute a command as the superuser or another user, as specified by the security policy. The invoking user's real (not effective) user ID is used to determine the user name with which to query the security policy.
sudo supports a plug-in architecture for security policies and input/output logging. Third parties can develop and distribute their own policy and I/O logging plug-ins to work seamlessly with the sudo front end. The default security policy is sudoers which is configured via the file /etc/sudoers and any entries in /etc/sudoers.d
The security policy determines what privileges, if any, a user has to run sudo The policy may require that users authenticate themselves with a password or another authentication mechanism. If authentication is required, sudo will exit if the user's password is not entered within a configurable time limit. This limit is policy-specific.

### Solution

First determine is LDAP functionality is required. If so, then install sudo-ldap else install sudo
Example:
# apt install sudo

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.5 |
| **800-171** | 3.1.6 |
| **800-171R3** | 03.01.06a. |
| **800-171R3** | 03.01.06b. |
| **800-53** | AC-6(2) |
| **800-53** | AC-6(5) |
| **800-53R5** | AC-6(2) |
| **800-53R5** | AC-6(5) |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.10.6(a) |
| **CSCV7** | 4.3 |
| **CSCV8** | 5.4 |
| **CSF** | PR.AC-4 |
| **CSF2.0** | PR.AA-05 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.8.2 |

| | |
|---|---|
| **ISO-27001-2022** | A.8.18 |
| **ISO/IEC-27001** | A.9.2.3 |
| **ITSG-33** | AC-6(2) |
| **ITSG-33** | AC-6(5) |
| **LEVEL** | 1A |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.6.1 |
| **NIAV2** | AM1 |
| **NIAV2** | AM23f |
| **NIAV2** | AM32 |
| **NIAV2** | AM33 |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | VL3a |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **SWIFT-CSCV1** | 1.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The command '/usr/bin/dpkg -s sudo sudo-ldap 2>&1' returned :

dpkg-query: package 'sudo-ldap' is not installed and no information is available
Package: sudo
Status: install ok installed
Priority: important
Section: admin
Installed-Size: 3464
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Architecture: amd64
Multi-Arch: foreign
Version: 1.9.15p5-3ubuntu5
Replaces: sudo-ldap
```

```
Depends: libapparmor1 (>= 2.7.0~beta1+bzr1772), libaudit1 (>= 1:2.2.1), libc6 (>= 2.38), libpam0g
 (>= 0.99.7.1), libselinux1 (>= 3.1~), libssl3t64 (>= 3.0.0), zlib1g (>= 1:1.2.0.2), libpam-
modules
Conflicts: sudo-ldap
Conffiles:
 /etc/pam.d/sudo b3a1b916bf62a2cc3280f7f9b94844ff
 /etc/pam.d/sudo-i ce9740f66cedf7716e26950abfe556fa
 /etc/sudo.conf 8c714b777580faea54a2eb6d5f17ad1d
 /etc/sudo_logsrvd.conf ad0ba586da300ae3ba46312ad744a6e2
 /etc/sudoers 8c20cd717552790f2312db0981337945
 /etc/sudoers.d/README bb1eba13940f331e91cfb9294d86a04f
Description: Provide limited super user privileges to specific users
 Sudo is a program designed to allow a sysadmin to give limited root
 privileges to users and log root activity.  The basic philosophy is to give
 as few privileges as possible but still allow people to get their work done.
 .
 This version is built with minimal shared library dependencies, use the
 sudo-ldap package instead if you need LDAP support for sudoers.
Homepage: https://www.sudo.ws/
Original-Maintainer: Sudo Maintainers <sudo@packages.debian.org>

Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

## 5.2.2 Ensure sudo commands use pty

### Info

sudo can be configured to run only from a pseudo terminal ( pseudo-pty ).
Attackers can run a malicious program using sudo which would fork a background process that remains even when the main program has finished executing.

### Solution

Edit the file /etc/sudoers with visudo or a file in /etc/sudoers.d/ with visudo -f <PATH TO FILE> and add the following line:
Defaults use_pty
Edit the file /etc/sudoers with visudo and any files in /etc/sudoers.d/ with visudo -f <PATH TO FILE> and remove any occurrence of !use_pty
Note:
- sudo will read each file in /etc/sudoers.d skipping file names that end in ~ or contain a character to avoid causing problems with package manager or editor temporary/backup files.
- Files are parsed in sorted lexical order. That is, /etc/sudoers.d/01_first will be parsed before /etc/sudoers.d/10_second
- Be aware that because the sorting is lexical, not numeric, /etc/sudoers.d/1_whoops would be loaded after /etc/sudoers.d/10_second
- Using a consistent number of leading zeroes in the file names can be used to avoid such problems.
Impact:
WARNING: Editing the sudo configuration incorrectly can cause sudo to stop functioning. Always use visudo to modify sudo configuration files.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.5 |
| **800-171** | 3.1.6 |
| **800-171R3** | 03.01.06a. |
| **800-171R3** | 03.01.06b. |
| **800-53** | AC-6(2) |
| **800-53** | AC-6(5) |
| **800-53R5** | AC-6(2) |
| **800-53R5** | AC-6(5) |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.10.6(a) |
| **CSCV7** | 5.1 |
| **CSCV8** | 5.4 |
| **CSF** | PR.AC-4 |
| **CSF2.0** | PR.AA-05 |
| **GDPR** | 32.1.b |

| | |
|---|---|
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.18 |
| **ISO/IEC-27001** | A.9.2.3 |
| **ITSG-33** | AC-6(2) |
| **ITSG-33** | AC-6(5) |
| **LEVEL** | 1A |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.6.1 |
| **NIAV2** | AM1 |
| **NIAV2** | AM23f |
| **NIAV2** | AM32 |
| **NIAV2** | AM33 |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | VL3a |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **SWIFT-CSCV1** | 1.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - /etc/sudoers use_pty
The command '/bin/grep -rPi -- '^\h*Defaults\h+([^#\n\r]+,\h*)?use_pty\b' /etc/sudoers*'
 returned :
```

```
/etc/sudoers:Defaults use_pty

-------------------------
PASSED - /etc/sudoers !use_pty
The command '/bin/grep -rPi -- '^\h*Defaults\h+([^#\n\r]+,\h*)?!use_pty\b' /etc/sudoers* | /bin/
awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}'' returned :

pass
```

## 5.2.5 Ensure re-authentication for privilege escalation is not disabled globally

### Info

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

### Solution

Configure the operating system to require users to reauthenticate for privilege escalation.
Based on the outcome of the audit procedure, use visudo -f <PATH TO FILE> to edit the relevant sudoers file.
Remove any occurrences of !authenticate tags in the file(s).

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.5 |
| **800-171** | 3.1.6 |
| **800-171R3** | 03.01.06a. |
| **800-171R3** | 03.01.06b. |
| **800-53** | AC-6(2) |
| **800-53** | AC-6(5) |
| **800-53R5** | AC-6(2) |
| **800-53R5** | AC-6(5) |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.10.6(a) |
| **CSCV7** | 4.3 |
| **CSCV8** | 5.4 |
| **CSF** | PR.AC-4 |
| **CSF2.0** | PR.AA-05 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.18 |
| **ISO/IEC-27001** | A.9.2.3 |

| | |
|---|---|
| **ITSG-33** | AC-6(2) |
| **ITSG-33** | AC-6(5) |
| **LEVEL** | 1A |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.6.1 |
| **NIAV2** | AM1 |
| **NIAV2** | AM23f |
| **NIAV2** | AM32 |
| **NIAV2** | AM33 |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | VL3a |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **SWIFT-CSCV1** | 1.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

### Assets

**linux_project**

```
The following file(s) do not contain "^[^#].*!authenticate":
      /etc/sudoers
      /etc/sudoers.d/90-cloud-init-users
      /etc/sudoers.d/README
```

## 5.2.6 Ensure sudo authentication timeout is configured correctly

### Info

sudo caches used credentials for a default of 15 minutes. This is for ease of use when there are multiple administrative tasks to perform. The timeout can be modified to suit local security policies.
This default is distribution specific. See audit section for further information.
Setting a timeout value reduces the window of opportunity for unauthorized privileged access to another user.

### Solution

If the currently configured timeout is larger than 15 minutes, edit the file listed in the audit section with visudo -f <PATH TO FILE> and modify the entry timestamp_timeout= to 15 minutes or less as per your site policy. The value is in minutes. This particular entry may appear on it's own, or on the same line as env_reset See the following two examples:
Defaults env_reset, timestamp_timeout=15 Defaults timestamp_timeout=15 Defaults env_reset

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.5 |
| **800-171** | 3.1.6 |
| **800-171R3** | 03.01.06a. |
| **800-171R3** | 03.01.06b. |
| **800-53** | AC-6(2) |
| **800-53** | AC-6(5) |
| **800-53R5** | AC-6(2) |
| **800-53R5** | AC-6(5) |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.10.6(a) |
| **CSCV7** | 4.3 |
| **CSCV8** | 5.4 |
| **CSF** | PR.AC-4 |
| **CSF2.0** | PR.AA-05 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.18 |

| | |
|---|---|
| **ISO/IEC-27001** | A.9.2.3 |
| **ITSG-33** | AC-6(2) |
| **ITSG-33** | AC-6(5) |
| **LEVEL** | 1A |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.6.1 |
| **NIAV2** | AM1 |
| **NIAV2** | AM23f |
| **NIAV2** | AM32 |
| **NIAV2** | AM33 |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | VL3a |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **SWIFT-CSCV1** | 1.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
One of the following must pass to satisfy this requirement:

-------------------------
PASSED - sudo timeout
The command '/bin/sudo -V | /bin/grep 'Authentication timestamp timeout:'' returned :

Authentication timestamp timeout: 15.0 minutes

-------------------------
PASSED - On disk timestamp_timeout
No matching files were found
```

## 5.3.1.1 Ensure latest version of pam is installed

### Info

Updated versions of PAM include additional functionality
To ensure the system has full functionality and access to the options covered by this Benchmark the latest version of libpam-runtime should be installed on the system

### Solution

- IF - the version of libpam-runtime on the system is less than version 1.5.3-5 :
Run the following command to update to the latest version of PAM :
# apt upgrade libpam-runtime

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

### Assets

#### linux_project

```
The command '/bin/dpkg -s libpam-runtime | /bin/grep -E '(Status:|Version)'' returned :

Status: install ok installed
Version: 1.5.3-5ubuntu5.1
```

## 5.3.1.2 Ensure libpam-modules is installed

### Info

Pluggable Authentication Modules for PAM
To ensure the system has full functionality and access to the PAM options covered by this Benchmark

### Solution

- IF - the version of libpam-modules on the system is less than version 1.5.3-5 :
Run the following command to update to the latest version of PAM :
# apt upgrade libpam-modules

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

### Assets

**linux_project**

```
The command '/bin/dpkg -s libpam-modules | /bin/grep -E '(Status:|Version)'' returned :

Status: install ok installed
Version: 1.5.3-5ubuntu5.1
```

## 5.3.2.1 Ensure pam_unix module is enabled

### Info

pam_unix is the standard Unix authentication module. It uses standard calls from the system's libraries to retrieve and set account information as well as authentication. Usually this is obtained from the /etc/passwd and if shadow is enabled, the /etc/shadow file as well.

The account component performs the task of establishing the status of the user's account and password based on the following shadow elements: expire last_change max_change min_change warn_change In the case of the latter, it may offer advice to the user on changing their password or, through the PAM_AUTHTOKEN_REQD return, delay giving service to the user until they have established a new password. The entries listed above are documented in the shadow(5) manual page. Should the user's record not contain one or more of these entries, the corresponding shadow check is not performed.

The authentication component performs the task of checking the users credentials (password). The default action of this module is to not permit the user access to a service if their official password is blank.

The system should only provide access after performing authentication of a user.

### Solution

Run the following command to enable the pam_unix module:

```
# pam-auth-update --enable unix
```

Note: If a site specific custom profile is being used in your environment to configure PAM that includes the configuration for the pam_faillock module, enable that module instead

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |

| | |
|---|---|
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |

| | |
|---|---|
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |

| | |
|---|---|
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - /etc/pam.d/common-password
Compliant file(s):
      /etc/pam.d/common-password - regex '^\h*password\h+[^#\n\r]+\h+pam_unix\.so\b' found -
 expect '^\h*password\h+[^#\n\r]+\h+pam_unix\.so\b' found in the following lines:
          25: password [success=1 default=ignore] pam_unix.so obscure yescrypt

-------------------------
PASSED - /etc/pam.d/common-account
Compliant file(s):
      /etc/pam.d/common-account - regex '^\h*account\h+[^#\n\r]+\h+pam_unix\.so\b' found - expect
 '^\h*account\h+[^#\n\r]+\h+pam_unix\.so\b' found in the following lines:
          17: account [success=1 new_authtok_reqd=done default=ignore] pam_unix.so

-------------------------
PASSED - /etc/pam.d/common-session
Compliant file(s):
      /etc/pam.d/common-session - regex '^\h*session\h+[^#\n\r]+\h+pam_unix\.so\b' found - expect
 '^\h*session\h+[^#\n\r]+\h+pam_unix\.so\b' found in the following lines:
          28: session required pam_unix.so

-------------------------
PASSED - /etc/pam.d/common-auth
Compliant file(s):
      /etc/pam.d/common-auth - regex '^\h*auth\h+[^#\n\r]+\h+pam_unix\.so\b' found - expect '^
\h*auth\h+[^#\n\r]+\h+pam_unix\.so\b' found in the following lines:
          17: auth [success=1 default=ignore] pam_unix.so nullok
```

## 5.3.3.4.2 Ensure pam_unix does not include remember

### Info

The remember=n argument saves the last n passwords for each user in /etc/security/opasswd in order to force password change history and keep the user from alternating between the same password too frequently. The MD5 password hash algorithm is used for storing the old passwords. Instead of this option the pam_pwhistory module should be used. The pam_pwhistory module saves the last n passwords for each user in /etc/security/opasswd using the password hash algorithm set on the pam_unix module. This allows for the yescrypt or sha512 hash algorithm to be used.
The remember=n argument should be removed to ensure a strong password hashing algorithm is being used. A stronger hash provides additional protection to the system by increasing the level of effort needed for an attacker to successfully determine local user's old passwords stored in /etc/security/opasswd

### Solution

Run the following command:
# grep -PH -- '^h*([^# r]+h+)?pam_unix.soh+([^# r]+h+)?rememberb' /usr/share/pam-configs/*
Edit any files returned and remove the remember=_<N>_ argument for the pam_unix lines
Example output:
[success=end default=ignore] pam_unix.so obscure use_authtok try_first_pass yescrypt remember=5 # **<- remove remember=<N>** [success=end default=ignore] pam_unix.so obscure yescrypt remember=5 # **<- remove remember=<N>**
Run the following command to update the files in the /etc/pam.d/ directory:
# pam-auth-update --enable <EDITED_PROFILE_NAME>
Example:
# pam-auth-update --enable unix
Note: If custom files are being used, the corresponding files in /etc/pam.d/ would need to be edited directly, and the pam-auth-update --enable <EDITED_PROFILE_NAME> command skipped

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |

| | |
|---|---|
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - /etc/pamd./common-session remember=
The following file(s) do not contain "(?i)^\h*^\h*[^#\n\r]+\h+pam_unix\.so\b[^#\n\r]+remember=
\b":
      /etc/pam.d/common-session

-------------------------
PASSED - /etc/pamd./common-password remember=
The following file(s) do not contain "(?i)^\h*^\h*[^#\n\r]+\h+pam_unix\.so\b[^#\n\r]+remember=
\b":
      /etc/pam.d/common-password

-------------------------
PASSED - /etc/pamd./common-session-noninteractive remember=
The following file(s) do not contain "(?i)^\h*^\h*[^#\n\r]+\h+pam_unix\.so\b[^#\n\r]+remember=
\b":
      /etc/pam.d/common-session-noninteractive

-------------------------
PASSED - /etc/pamd./common-auth remember=
The following file(s) do not contain "(?i)^\h*^\h*[^#\n\r]+\h+pam_unix\.so\b[^#\n\r]+remember=
\b":
      /etc/pam.d/common-auth

-------------------------
PASSED - /etc/pamd./common-account remember=
The following file(s) do not contain "(?i)^\h*^\h*[^#\n\r]+\h+pam_unix\.so\b[^#\n\r]+remember=
\b":
      /etc/pam.d/common-account
```

## 5.3.3.4.3 Ensure pam_unix includes a strong password hashing algorithm

### Info

A cryptographic hash function converts an arbitrary-length input into a fixed length output. Password hashing performs a one-way transformation of a password, turning the password into another string, called the hashed password.
The pam_unix module can be configured to use one of the following hashing algorithms for user's passwords:
- md5 - When a user changes their password next, encrypt it with the MD5 algorithm.
- bigcrypt - When a user changes their password next, encrypt it with the DEC C2 algorithm.
- sha256 - When a user changes their password next, encrypt it with the SHA256 algorithm. The SHA256 algorithm must be supported by the crypt(3) function.
- sha512 - When a user changes their password next, encrypt it with the SHA512 algorithm. The SHA512 algorithm must be supported by the crypt(3) function.
- blowfish - When a user changes their password next, encrypt it with the blowfish algorithm. The blowfish algorithm must be supported by the crypt(3) function.
- gost_yescrypt - When a user changes their password next, encrypt it with the gost-yescrypt algorithm. The gost-yescrypt algorithm must be supported by the crypt(3) function.
- yescrypt - When a user changes their password next, encrypt it with the yescrypt algorithm. The yescrypt algorithm must be supported by the crypt(3) function.

The SHA-512 and yescrypt algorithms provide a stronger hash than other algorithms used by Linux for password hash generation. A stronger hash provides additional protection to the system by increasing the level of effort needed for an attacker to successfully determine local user passwords.
Note: These changes only apply to the local system.

### Solution

Run the following command:
# awk '/Password-Type:/{ f = 1;next } /-Type:/{ f = 0 } f {if (/pam_unix.so/) print FILENAME}' /usr/share/pam-configs/*
Edit any returned files and edit or add a strong hashing algorithm, either sha512 or yescrypt, that meets local site policy to the pam_unix lines in the Password section:
Example File:
Name: Unix authentication Default: yes Priority: 256 Auth-Type: Primary # <- Start of "Auth" section Auth:
[success=end default=ignore] pam_unix.so try_first_pass Auth-Initial:
[success=end default=ignore] pam_unix.so Account-Type: Primary # <- Start of "Account" section Account:
[success=end new_authtok_reqd=done default=ignore] pam_unix.so Account-Initial:
[success=end new_authtok_reqd=done default=ignore] pam_unix.so Session-Type: Additional # <- Start of "Session" section Session:
required pam_unix.so Session-Initial:
required pam_unix.so Password-Type: Primary # <- Start of "Password" section Password:
[success=end default=ignore] pam_unix.so obscure use_authtok try_first_pass yescrypt # <- **ensure hashing algorithm is either sha512 or yescrypt** Password-Initial:
[success=end default=ignore] pam_unix.so obscure yescrypt # <- **ensure hashing algorithm is either sha512 or yescrypt**
Run the following command to update the files in the /etc/pam.d/ directory:
# pam-auth-update --enable <MODIFIED_PROFILE_NAME>
Example:
# pam-auth-update --enable unix

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171** | 3.13.16 |
| **800-171R3** | 03.05.07 |
| **800-171R3** | 03.13.08 |
| **800-53** | IA-5(1) |
| **800-53** | SC-28 |
| **800-53** | SC-28(1) |

| | |
|---|---|
| **800-53R5** | IA-5(1) |
| **800-53R5** | SC-28 |
| **800-53R5** | SC-28(1) |
| **CN-L3** | 8.1.4.7(b) |
| **CN-L3** | 8.1.4.8(b) |
| **CSCV7** | 16.4 |
| **CSCV8** | 3.11 |
| **CSF** | PR.AC-1 |
| **CSF** | PR.DS-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **CSF2.0** | PR.DS-01 |
| **GDPR** | 32.1.a |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(a)(2)(iv) |
| **HIPAA** | 164.312(d) |
| **HIPAA** | 164.312(e)(2)(ii) |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ISO-27001-2022** | A.5.33 |
| **ITSG-33** | IA-5(1) |
| **ITSG-33** | SC-28 |
| **ITSG-33** | SC-28a. |
| **ITSG-33** | SC-28(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **PCI-DSSV3.2.1** | 3.4 |
| **PCI-DSSV4.0** | 3.3.2 |

| | |
|---|---|
| **PCI-DSSV4.0** | 3.5.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |
| **TBA-FIISB** | 28.1 |

## Assets

### linux_project

```
Compliant file(s):
      /etc/pam.d/common-password - regex '(?i)^\h*password\h+([^#\n\r]+)\h+pam_unix\.so\h+([^#\n
\r]+\h+)?(SHA512|YESCRYPT)\b' found - expect '(?i)^\h*password\h+([^#\n\r]+)\h+pam_unix\.so\h+([^#
\n\r]+\h+)?(SHA512|YESCRYPT)\b' found in the following lines:
          25: password [success=1 default=ignore] pam_unix.so obscure yescrypt
```

## 5.4.1.3 Ensure password expiration warning days is configured

### Info

The PASS_WARN_AGE parameter in /etc/login.defs allows an administrator to notify users that their password will expire in a defined number of days.
PASS_WARN_AGE
<N>
- The number of days warning given before a password expires. A zero means warning is given only upon the day of expiration, a negative value means no warning is given. If not specified, no warning will be provided.
Providing an advance warning that a password will be expiring gives users time to think of a secure password. Users caught unaware may choose a simple password or write it down where it may be discovered.

### Solution

Edit /etc/login.defs and set PASS_WARN_AGE to a value of 7 or more that follows local site policy:
Example:
```
PASS_WARN_AGE 7
```
Run the following command to modify user parameters for all users with a password set to a minimum warning to 7 or more days that follows local site policy:
```
# chage --warndays <N> <user>
```
Example:
```
# awk -F: '($2~/^$.+$/) {if($6 < 7)system ("chage --warndays 7 " $1)}' /etc/shadow
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.1 |
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171** | 3.13.1 |
| **800-171** | 3.13.2 |
| **800-171R3** | 03.04.01 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-171R3** | 03.16.01 |
| **800-53** | CM-2 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53** | CM-7(1) |
| **800-53** | CM-9 |
| **800-53** | SA-3 |
| **800-53** | SA-8 |
| **800-53** | SA-10 |
| **800-53R5** | CM-1 |

| | |
|---|---|
| **800-53R5** | CM-2 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **800-53R5** | CM-7(1) |
| **800-53R5** | CM-9 |
| **800-53R5** | SA-3 |
| **800-53R5** | SA-8 |
| **800-53R5** | SA-10 |
| **CSCV7** | 4.4 |
| **CSCV8** | 4.1 |
| **CSF** | DE.AE-1 |
| **CSF** | PR.DS-7 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.IP-2 |
| **CSF** | PR.IP-3 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | ID.AM-08 |
| **CSF2.0** | ID.IM-01 |
| **CSF2.0** | ID.IM-02 |
| **CSF2.0** | ID.IM-03 |
| **CSF2.0** | ID.RA-09 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-03 |
| **CSF2.0** | PR.PS-01 |
| **CSF2.0** | PR.PS-06 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.2 |
| **ISO-27001-2022** | A.5.8 |
| **ISO-27001-2022** | A.8.9 |

| | |
|---|---|
| **ISO-27001-2022** | A.8.25 |
| **ISO-27001-2022** | A.8.26 |
| **ISO-27001-2022** | A.8.27 |
| **ISO-27001-2022** | A.8.28 |
| **ISO-27001-2022** | A.8.30 |
| **ISO-27001-2022** | A.8.31 |
| **ISO-27001-2022** | A.8.32 |
| **ITSG-33** | CM-2 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **ITSG-33** | CM-7(1) |
| **ITSG-33** | CM-9 |
| **ITSG-33** | SA-3 |
| **ITSG-33** | SA-8 |
| **ITSG-33** | SA-8a. |
| **ITSG-33** | SA-10 |
| **LEVEL** | 1A |
| **NESA** | T1.2.1 |
| **NESA** | T1.2.2 |
| **NESA** | T3.2.5 |
| **NESA** | T3.4.1 |
| **NESA** | T4.5.3 |
| **NESA** | T4.5.4 |
| **NESA** | T7.2.1 |
| **NESA** | T7.5.1 |
| **NESA** | T7.5.3 |
| **NESA** | T7.6.1 |
| **NESA** | T7.6.2 |
| **NESA** | T7.6.3 |
| **NESA** | T7.6.5 |
| **NIAV2** | SS3 |

| | |
|---|---|
| **NIAV2** | SS15a |
| **NIAV2** | SS16 |
| **NIAV2** | VL2 |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - shadow password warn days
The command '/bin/awk -F: '($2~/^\$.+\$/) {if($6 < 7)print "User: " $1 " PASS_WARN_AGE: " $6}' /
etc/shadow | /bin/awk '{print} END {if (NR == 0) print "pass"; else print "fail"}'' returned :

pass

-------------------------
PASSED - login.defs - PASS_WARN_AGE
Compliant file(s):
      /etc/login.defs - regex '(?i)^\h*PASS_WARN_AGE\h+\d+\b' found - expect '(?i)^
\h*PASS_WARN_AGE\h+7\b' found in the following lines:
          167: PASS_WARN_AGE 7
```

## 5.4.1.4 Ensure strong password hashing algorithm is configured

### Info

A cryptographic hash function converts an arbitrary-length input into a fixed length output. Password hashing performs a one-way transformation of a password, turning the password into another string, called the hashed password.
ENCRYPT_METHOD (string) - This defines the system default encryption algorithm for encrypting passwords (if no algorithm are specified on the command line). It can take one of these values:
- MD5 - MD5-based algorithm will be used for encrypting password
- SHA256 - SHA256-based algorithm will be used for encrypting password
- SHA512 - SHA512-based algorithm will be used for encrypting password
- BCRYPT - BCRYPT-based algorithm will be used for encrypting password
- YESCRYPT - YESCRYPT-based algorithm will be used for encrypting password
- DES - DES-based algorithm will be used for encrypting password (default)

Note:
- This parameter overrides the deprecated MD5_CRYPT_ENAB variable.
- This parameter will only affect the generation of group passwords.
- The generation of user passwords is done by PAM and subject to the PAM configuration.
- It is recommended to set this variable consistently with the PAM configuration.

The SHA-512 and yescrypt algorithms provide a stronger hash than other algorithms used by Linux for password hash generation. A stronger hash provides additional protection to the system by increasing the level of effort needed for an attacker to successfully determine local group passwords.

### Solution

Edit /etc/login.defs and set the ENCRYPT_METHOD to SHA512 or YESCRYPT :
ENCRYPT_METHOD <HASHING_ALGORITHM>
Example:
ENCRYPT_METHOD YESCRYPT
Note:
- This only effects local groups' passwords created after updating the file to use sha512 or yescrypt
- If it is determined that the password algorithm being used is not sha512 or yescrypt once it is changed, it is recommended that all group passwords be updated to use the stronger hashing algorithm.
- It is recommended that the chosen hashing algorithm is consistent across /etc/login.defs and the PAM configuration

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171** | 3.13.16 |
| **800-171R3** | 03.05.07 |
| **800-171R3** | 03.13.08 |
| **800-53** | IA-5(1) |
| **800-53** | SC-28 |
| **800-53** | SC-28(1) |
| **800-53R5** | IA-5(1) |
| **800-53R5** | SC-28 |
| **800-53R5** | SC-28(1) |
| **CN-L3** | 8.1.4.7(b) |
| **CN-L3** | 8.1.4.8(b) |
| **CSCV7** | 16.4 |

| | |
|---|---|
| **CSCV8** | 3.11 |
| **CSF** | PR.AC-1 |
| **CSF** | PR.DS-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **CSF2.0** | PR.DS-01 |
| **GDPR** | 32.1.a |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(a)(2)(iv) |
| **HIPAA** | 164.312(d) |
| **HIPAA** | 164.312(e)(2)(ii) |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ISO-27001-2022** | A.5.33 |
| **ITSG-33** | IA-5(1) |
| **ITSG-33** | SC-28 |
| **ITSG-33** | SC-28a. |
| **ITSG-33** | SC-28(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **PCI-DSSV3.2.1** | 3.4 |
| **PCI-DSSV4.0** | 3.3.2 |
| **PCI-DSSV4.0** | 3.5.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |
| **TBA-FIISB** | 28.1 |

### Assets

### linux_project

```
Compliant file(s):
      /etc/login.defs - regex '^\s*ENCRYPT_METHOD\s+' found - expect '^\s*ENCRYPT_METHOD\s+(?i)
(SHA512|YESCRYPT)(?-i)\s*$' found in the following lines:
          295: ENCRYPT_METHOD SHA512
```

## 5.4.1.6 Ensure all users last password change date is in the past

### Info

All users should have a password change date in the past.
If a user's recorded password change date is in the future, then they could bypass any set password expiration.

### Solution

Investigate any users with a password change date in the future and correct them. Locking the account, expiring the password, or resetting the password manually may be appropriate.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

### Assets

#### linux_project

```
The command script with multiple lines returned :

Pass
```

## 5.4.2.1 Ensure root is the only UID 0 account

### Info

Any account with UID 0 has superuser privileges on the system.
This access must be limited to only the default root account and only from the system console. Administrative access must be through an unprivileged account using an approved mechanism as noted in Item 5.6 Ensure access to the su command is restricted.

### Solution

Run the following command to change the root account UID to 0 :
# usermod -u 0 root
Modify any users other than root with UID 0 and assign them a new UID.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.5 |
| **800-171R3** | 03.01.06a. |
| **800-53** | AC-6(5) |
| **800-53R5** | AC-6(5) |
| **CN-L3** | 8.1.10.6(a) |
| **CSF** | PR.AC-4 |
| **CSF2.0** | PR.AA-05 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.18 |
| **ISO/IEC-27001** | A.9.2.3 |
| **ITSG-33** | AC-6(5) |
| **LEVEL** | 1A |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.6.1 |
| **NIAV2** | AM32 |
| **NIAV2** | AM33 |
| **NIAV2** | VL3a |
| **PCI-DSSV3.2.1** | 7.1.2 |

| | |
|---|---|
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **SWIFT-CSCV1** | 1.2 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
No issues found.
```

## 5.4.2.2 Ensure root is the only GID 0 account

### Info

The usermod command can be used to specify which group the root account belongs to. This affects permissions of files that are created by the root account.
Using GID 0 for the root account helps prevent root -owned files from accidentally becoming accessible to non-privileged users.

### Solution

Run the following command to set the root user's GID to 0 :
# usermod -g 0 root
Run the following command to set the root group's GID to 0 :
# groupmod -g 0 root
Remove any users other than the root user with GID 0 or assign them a new GID if appropriate.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |

| | |
|---|---|
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |

| | |
|---|---|
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |

|  |  |
|---|---|
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **
 - * Correctly configured * :
  - No unauthorized user's GID is: "0"
  - User "root" GID is correctly set to: "0"
```

## 5.4.2.3 Ensure group root is the only GID 0 group

### Info

The groupmod command can be used to specify which group the root group belongs to. This affects permissions of files that are group owned by the root group.
Using GID 0 for the root group helps prevent root group owned files from accidentally becoming accessible to non-privileged users.

### Solution

Run the following command to set the root group's GID to 0 :

```
# groupmod -g 0 root
```

Remove any groups other than the root group with GID 0 or assign them a new GID if appropriate.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |

| | |
|---|---|
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |

| | |
|---|---|
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |

|  |  |
|---|---|
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
No issues found.
```

## 5.4.2.4 Ensure root account access is controlled

### Info

There are a number of methods to access the root account directly. Without a password set any user would be able to gain access and thus control over the entire system.
Access to root should be secured at all times.

### Solution

Run the following command to set a password for the root user:
# passwd root
- OR -
Run the following command to lock the root user account:
# usermod -L root
Impact:
If there are any automated processes that relies on access to the root account without authentication, they will fail after remediation.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |

| | |
|---|---|
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |

| | |
|---|---|
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |

|  |  |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The command '/bin/passwd -S root | /bin/awk '$2 ~ /^(P|L)/ {print "User: \"" $1 "\" Password is
 status: " $2}'' returned :

User: "root" Password is status: P
```

## 5.4.2.6 Ensure root user umask is configured

### Info

The user file-creation mode mask ( umask ) is used to determine the file permission for newly created directories and files. In Linux, the default permissions for any newly created directory is 0777 ( rwxrwxrwx ), and for any newly created file it is 0666 ( rw-rw-rw- ). The umask modifies the default Linux permissions by restricting (masking) these permissions. The umask is not simply subtracted, but is processed bitwise. Bits set in the umask are cleared in the resulting file mode.
umask can be set with either Octal or Symbolic values:
- Octal (Numeric) Value - Represented by either three or four digits. ie umask 0027 or umask 027 If a four digit umask is used, the first digit is ignored. The remaining three digits effect the resulting permissions for user, group, and world/other respectively.
- Symbolic Value - Represented by a comma separated list for User u group g and world/other o The permissions listed are not masked by umask ie a umask set by umask u=rwx,g=rx,o= is the Symbolic equivalent of the Octal umask 027 This umask would set a newly created directory with file mode drwxr-x--- and a newly created file with file mode rw-r-----
root user Shell Configuration Files:
- /root/.bash_profile - Is executed to configure the root users' shell before the initial command prompt. Is only read by login shells.
- /root/.bashrc - Is executed for interactive shells. only read by a shell that's both interactive and non-login
umask is set by order of precedence. If umask is set in multiple locations, this order of precedence will determine the system's default umask
Order of precedence:
- /root/.bash_profile
- /root/.bashrc
- The system default umask
Setting a secure value for umask ensures that users make a conscious choice about their file permissions. A permissive umask value could result in directories or files with excessive permissions that can be read and/or written to by unauthorized users.

### Solution

Edit /root/.bash_profile and /root/.bashrc and remove, comment out, or update any line with umask to be 0027 or more restrictive.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |

| | |
|---|---|
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |

| | |
|---|---|
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |

| | |
|---|---|
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The following file(s) do not contain "(?i)^\h*umask\h+(([0-7][0-7][01][0-7]\b|[0-7][0-7][0-7]
[0-6]\b)|([0-7][01][0-7]\b|[0-7][0-7][0-6]\b)|(u=[rwx]{1,3},)?(((g=[rx]?[rx]?w[rx]?[rx]?\b)
(,o=[rwx]{1,3})?)|((g=[wrx]{1,3},)?o=[wrx]{1,3}\b)))":
      /root/.bashrc
```

## 5.4.2.7 Ensure system accounts do not have a valid login shell

### Info

There are a number of accounts provided with most distributions that are used to manage applications and are not intended to provide an interactive shell. Furthermore, a user may add special accounts that are not intended to provide an interactive shell.

It is important to make sure that accounts that are not being used by regular users are prevented from being used to provide an interactive shell. By default, most distributions set the password field for these accounts to an invalid string, but it is also recommended that the shell field in the password file be set to the nologin shell. This prevents the account from potentially being used to run any commands.

### Solution

Run the following command to set the shell for any service accounts returned by the audit to nologin :

```
# usermod -s $(command -v nologin) <user>
```

Example script:

```
#!/usr/bin/env bash
{ l_valid_shells="^($( awk -F/ '$NF != "nologin" {print}' /etc/shells | sed -rn '/^//{s,/,\\/,g;p}' | paste -s -d '|' - ))$"
awk -v pat="$l_valid_shells" -F: '($1!~/^(root|halt|sync|shutdown|nfsnobody)$/ && ($3<'"$(awk '/^s*UID_MIN/{print
$2}' /etc/login.defs)"' || $3 == 65534) && $(NF) ~ pat) {system ("usermod -s '"$(command -v nologin)"' " $1)}' /etc/
passwd }
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |

| | |
|---|---|
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |

| | |
|---|---|
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |

| | |
|---|---|
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

pass
```

## 5.4.2.8 Ensure accounts without a valid login shell are locked

### Info

There are a number of accounts provided with most distributions that are used to manage applications and are not intended to provide an interactive shell. Furthermore, a user may add special accounts that are not intended to provide an interactive shell.

It is important to make sure that accounts that are not being used by regular users are prevented from being used to provide an interactive shell. By default, most distributions set the password field for these accounts to an invalid string, but it is also recommended that the shell field in the password file be set to the nologin shell. This prevents the account from potentially being used to run any commands.

### Solution

Run the following command to lock any non-root accounts without a valid login shell returned by the audit:

```
# usermod -L <user>
```

Example script:

```
:
#!/usr/bin/env bash
{ l_valid_shells="^($(awk -F/ '$NF != "nologin" {print}' /etc/shells | sed -rn '/^\//{s,/,\\/,g;p}' | paste -s -d '|' - ))$"
while IFS= read -r l_user; do passwd -S "$l_user" | awk '$2 !~ /^L/ {system ("usermod -L " $1)}'
done < <(awk -v pat="$l_valid_shells" -F: '($1 != "root" && $(NF) !~ pat) {print $1}' /etc/passwd) }
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |

| | |
|---|---|
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |

| | |
|---|---|
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |

| | |
|---|---|
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

pass
```

## 6.1.1.1 Ensure journald service is enabled and active

### Info

Ensure that the systemd-journald service is enabled to allow capturing of logging events.
If the systemd-journald service is not enabled to start on boot, the system will not capture logging events.

### Solution

Run the following commands to unmask and start systemd-journald.service

```
# systemctl unmask systemd-journald.service # systemctl start systemd-journald.service
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171** | 3.3.6 |
| **800-171R3** | 03.03.01 |
| **800-171R3** | 03.03.03 |
| **800-171R3** | 03.03.06a. |
| **800-53** | AU-2 |
| **800-53** | AU-7 |
| **800-53** | AU-12 |
| **800-53R5** | AU-2 |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-12 |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 8.1.4.3(a) |
| **CSCV7** | 6.2 |
| **CSCV7** | 6.3 |
| **CSCV8** | 8.2 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | DE.CM-7 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |

| | |
|---|---|
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.8.15 |
| **ITSG-33** | AU-2 |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-12 |
| **LEVEL** | 1A |
| **NESA** | M1.2.2 |
| **NESA** | M5.5.1 |
| **NIAV2** | AM7 |
| **NIAV2** | AM11a |
| **NIAV2** | AM11b |
| **NIAV2** | AM11c |
| **NIAV2** | AM11d |
| **NIAV2** | AM11e |
| **NIAV2** | SS30 |
| **NIAV2** | VL8 |
| **PCI-DSSV3.2.1** | 10.1 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |

### Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - journald active
The command '/bin/systemctl is-active systemd-journald.service' returned :

active

-------------------------
PASSED - journald check - enabled
The command '/bin/systemctl is-enabled systemd-journald.service' returned :

static
```

## 6.1.1.2 Ensure journald log file access is configured

### Info

Journald will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.
It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

### Solution

If the default configuration is not appropriate for the site specific requirements, copy /usr/lib/tmpfiles.d/systemd.conf to /etc/tmpfiles.d/systemd.conf and modify as required. Recommended mode for logfiles is 0640 or more restrictive.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |

| | |
|---|---|
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |

| | |
|---|---|
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1M |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |

| | |
|---|---|
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
 The command script with multiple lines returned :

- Audit Result:
  ** PASS **
 - File: "/usr/lib/tmpfiles.d/systemd.conf" sets:
  - Directory "/run/user" access is:
    mode: "0755", owned by: "root", and group owned by: "root"
  - Directory "/run/systemd/ask-password" access is:
    mode: "0755", owned by: "root", and group owned by: "root"
  - Directory "/run/systemd/seats" access is:
    mode: "0755", owned by: "root", and group owned by: "root"
  - Directory "/run/systemd/sessions" access is:
    mode: "0755", owned by: "root", and group owned by: "root"
  - Directory "/run/systemd/users" access is:
    mode: "0755", owned by: "root", and group owned by: "root"
  - Directory "/run/systemd/machines" access is:
    mode: "0755", owned by: "root", and group owned by: "root"
  - Directory "/run/systemd/shutdown" access is:
    mode: "0755", owned by: "root", and group owned by: "root"
  - Directory "/run/log" access is:
    mode: "0755", owned by: "root", and group owned by: "root"
  - Directory "/var/lib/systemd" access is:
    mode: "0755", owned by: "root", and group owned by: "root"
  - Directory "/var/lib/systemd/coredump" access is:
    mode: "0755", owned by: "root", and group owned by: "root"
  - Directory "/var/lib/systemd/ephemeral-trees" access is:
    mode: "0755", owned by: "root", and group owned by: "root"
  - Directory "/var/lib/private" access is:
    mode: "0700", owned by: "root", and group owned by: "root"
  - Directory "/var/log/private" access is:
    mode: "0700", owned by: [...]
```

## 6.1.1.4 Ensure only one logging system is in use

### Info

Best practices recommend that a single centralized logging system be used for log management, choose a single service either rsyslog - OR - journald to be used as a single centralized logging system.
Configuring only one logging service either rsyslog - OR - journald avoids redundancy, optimizes resources, simplifies configuration and management, and ensures consistency.

### Solution

- Determine whether to use journald - OR - rsyslog depending on site needs
- Configure systemd-jounald.service
- Configure only ONE either journald - OR - rsyslog and complete the recommendations in that subsection
- Return to this recommendation to ensure only one logging system is in use

Impact:
Transitioning from one logging service to another can be complex and time consuming, it involves reconfiguration and may result in data loss if not managed and reconfigured correctly.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171R3** | 03.03.01 |
| **800-53** | AU-2 |
| **800-53R5** | AU-2 |
| **CN-L3** | 8.1.4.3(a) |
| **CSF** | PR.PT-1 |
| **CSF2.0** | PR.PS-04 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.8.15 |
| **ITSG-33** | AU-2 |
| **LEVEL** | 1A |
| **NESA** | M1.2.2 |
| **NESA** | M5.5.1 |
| **NIAV2** | AM7 |
| **NIAV2** | AM11a |
| **NIAV2** | AM11b |
| **NIAV2** | AM11c |
| **NIAV2** | AM11d |

| | |
|---|---|
| **NIAV2** | AM11e |
| **NIAV2** | SS30 |
| **NIAV2** | VL8 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
 ** PASS **

 - rsyslog is in use
- follow the recommendations in Configure rsyslog subsection only
```

## 6.1.2.1.4 Ensure systemd-journal-remote service is not in use

### Info

Journald systemd-journal-remote supports the ability to receive messages from remote hosts, thus acting as a log server. Clients should not receive data from other hosts.
Note:
- The same package, systemd-journal-remote is used for both sending logs to remote hosts and receiving incoming logs.
- With regards to receiving logs, there are two services; systemd-journal-remote.socket and systemd-journal-remote.service
If a client is configured to also receive data, thus turning it into a server, the client system is acting outside it's operational boundary.
Note: This recommendation only applies if journald is the chosen method for client side logging Do not apply this recommendation if rsyslog is used.

### Solution

Run the following commands to stop and mask systemd-journal-remote.socket and systemd-journal-remote.service:
# systemctl stop systemd-journal-remote.socket systemd-journal-remote.service # systemctl mask systemd-journal-remote.socket systemd-journal-remote.service

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |

| | |
|---|---|
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - journald remote active
The command '/bin/systemctl is-active systemd-journal-remote.socket systemd-journal-remote.service
 | /bin/grep -P -- '^active' | /bin/awk '{print} END {if(NR==0) print "pass"}'' returned :

pass

-------------------------
PASSED - journald remote enabled
The command '/bin/systemctl is-enabled systemd-journal-remote.socket systemd-journal-
remote.service | /bin/grep -P -- '^enabled' | /bin/awk '{print} END {if(NR==0) print "pass"}''
 returned :

pass
```

## 6.1.3.1 Ensure rsyslog is installed

### Info

The rsyslog software is recommended in environments where journald does not meet operation requirements.
The security enhancements of rsyslog such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server) justify installing and configuring the package.

### Solution

Run the following command to install rsyslog :
# apt install rsyslog

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171** | 3.3.6 |
| **800-171R3** | 03.03.01 |
| **800-171R3** | 03.03.03 |
| **800-171R3** | 03.03.06a. |
| **800-53** | AU-2 |
| **800-53** | AU-7 |
| **800-53** | AU-12 |
| **800-53R5** | AU-2 |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-12 |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 8.1.4.3(a) |
| **CSCV7** | 6.2 |
| **CSCV7** | 6.3 |
| **CSCV8** | 8.2 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | DE.CM-7 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | DE.CM-01 |

| | |
|---|---|
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.8.15 |
| **ITSG-33** | AU-2 |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-12 |
| **LEVEL** | 1A |
| **NESA** | M1.2.2 |
| **NESA** | M5.5.1 |
| **NIAV2** | AM7 |
| **NIAV2** | AM11a |
| **NIAV2** | AM11b |
| **NIAV2** | AM11c |
| **NIAV2** | AM11d |
| **NIAV2** | AM11e |
| **NIAV2** | SS30 |
| **NIAV2** | VL8 |
| **PCI-DSSV3.2.1** | 10.1 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |

| | |
|---|---|
| **SWIFT-CSCV1** | 6.4 |

## Assets

### linux_project

```
The command '/bin/dpkg -s rsyslog 2>&1 | /bin/grep -E '(^Status:|not installed)'' returned :

Status: install ok installed
```

## 6.1.3.2 Ensure rsyslog service is enabled and active

### Info

Once the rsyslog package is installed, ensure that the service is enabled.
If the rsyslog service is not enabled to start on boot, the system will not capture logging events.

### Solution

- IF - rsyslog is being used for logging on the system:
Run the following commands to unmask, enable, and start rsyslog.service :

```
# systemctl unmask rsyslog.service # systemctl enable rsyslog.service # systemctl start rsyslog.service
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171** | 3.3.6 |
| **800-171R3** | 03.03.01 |
| **800-171R3** | 03.03.03 |
| **800-171R3** | 03.03.06a. |
| **800-53** | AU-2 |
| **800-53** | AU-7 |
| **800-53** | AU-12 |
| **800-53R5** | AU-2 |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-12 |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 8.1.4.3(a) |
| **CSCV7** | 6.2 |
| **CSCV7** | 6.3 |
| **CSCV8** | 8.2 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | DE.CM-7 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |

| | |
|---|---|
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.8.15 |
| **ITSG-33** | AU-2 |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-12 |
| **LEVEL** | 1A |
| **NESA** | M1.2.2 |
| **NESA** | M5.5.1 |
| **NIAV2** | AM7 |
| **NIAV2** | AM11a |
| **NIAV2** | AM11b |
| **NIAV2** | AM11c |
| **NIAV2** | AM11d |
| **NIAV2** | AM11e |
| **NIAV2** | SS30 |
| **NIAV2** | VL8 |
| **PCI-DSSV3.2.1** | 10.1 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |

**Assets**

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - enabled
The command '/bin/systemctl is-enabled rsyslog' returned :

enabled

-------------------------
PASSED - active
The command '/bin/systemctl is-active rsyslog' returned :

active
```

## 6.1.3.3 Ensure journald is configured to send logs to rsyslog

### Info

Data from systemd-journald may be stored in volatile memory or persisted locally on the server. Utilities exist to accept remote export of systemd-journald logs, however, use of the rsyslog service provides a consistent means of log collection and export.
- IF - rsyslog is the preferred method for capturing logs, all logs of the system should be sent to it for further processing.
Note: This recommendation only applies if rsyslog is the chosen method for client side logging Do not apply this recommendation if systemd-journald is used.

### Solution

- IF - Journald is the preferred method for capturing logs, this section and Recommendation should be skipped and the "Configure Journald" section followed.
- IF - rsyslog is the preferred method for capturing logs:
Set the following parameter in the [Journal] section in /etc/systemd/journald.conf or a file in /etc/systemd/journald.conf.d/ ending inconf :

```
ForwardToSyslog=yes
```

Example script to create systemd drop-in configuration file:

```
#!/usr/bin/env bash
{ a_settings=("ForwardToSyslog=yes") [ ! -d /etc/systemd/journald.conf.d/ ] && mkdir /etc/systemd/journald.conf.d/
if grep -Psq -- '^h*[Journal]' /etc/systemd/journald.conf.d/60-journald.conf; then printf '%s ' "" "${a_settings[@]}"
>> /etc/systemd/journald.conf.d/60-journald.conf else printf '%s ' "" "[Journal]" "${a_settings[@]}" >> /etc/systemd/journald.conf.d/60-journald.conf fi }
```

Note: If this setting appears in a canonically later file, or later in the same file, the setting will be overwritten
Run to following command to update the parameters in the service:
Restart systemd-journald.service :

```
# systemctl reload-or-restart systemd-journald.service
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171** | 3.3.5 |
| **800-171** | 3.3.6 |
| **800-171R3** | 03.03.01 |
| **800-171R3** | 03.03.03 |
| **800-171R3** | 03.03.05c. |
| **800-171R3** | 03.03.06a. |
| **800-53** | AU-2 |
| **800-53** | AU-6(3) |
| **800-53** | AU-7 |
| **800-53** | AU-12 |
| **800-53R5** | AU-2 |
| **800-53R5** | AU-6(3) |
| **800-53R5** | AU-7 |

| | |
|---|---|
| **800-53R5** | AU-12 |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 7.1.3.3(d) |
| **CN-L3** | 8.1.4.3(a) |
| **CSCV7** | 6.2 |
| **CSCV7** | 6.3 |
| **CSCV7** | 6.5 |
| **CSCV8** | 8.2 |
| **CSCV8** | 8.9 |
| **CSF** | DE.AE-2 |
| **CSF** | DE.AE-3 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | DE.CM-7 |
| **CSF** | DE.DP-4 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-1 |
| **CSF** | RS.AN-3 |
| **CSF** | RS.CO-2 |
| **CSF2.0** | DE.AE-02 |
| **CSF2.0** | DE.AE-03 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |

| | |
|---|---|
| **ISO-27001-2022** | A.5.25 |
| **ISO-27001-2022** | A.6.8 |
| **ISO-27001-2022** | A.8.15 |
| **ITSG-33** | AU-2 |
| **ITSG-33** | AU-6(3) |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-12 |
| **LEVEL** | 1A |
| **NESA** | M1.2.2 |
| **NESA** | M5.2.5 |
| **NESA** | M5.5.1 |
| **NIAV2** | AM7 |
| **NIAV2** | AM11a |
| **NIAV2** | AM11b |
| **NIAV2** | AM11c |
| **NIAV2** | AM11d |
| **NIAV2** | AM11e |
| **NIAV2** | SS30 |
| **NIAV2** | VL8 |
| **PCI-DSSV3.2.1** | 10.1 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - Ensure ForwardToSyslog set to yes
The command script with multiple lines returned :
```

```
- Audit Result:
  ** PASS **
  - Parameter: "ForwardToSyslog"
    correctly set to: "yes"
    in the file: "/usr/lib/systemd/journald.conf.d/syslog.conf"

-------------------------
PASSED - systemd-journald.service
The command '/bin/systemctl list-units --type service | grep -P -- '(journald|rsyslog)''
 returned :

rsyslog.service                                 loaded active running System Logging Service
  systemd-journald.service                        loaded active running Journal Service

-------------------------
PASSED - rsyslog.service
The command '/bin/systemctl list-units --type service | grep -P -- '(journald|rsyslog)''
 returned :

rsyslog.service                                 loaded active running System Logging Service
  systemd-journald.service                        loaded active running Journal Service
```

## 6.1.3.4 Ensure rsyslog log file creation mode is configured

### Info

rsyslog will create logfiles that do not already exist on the system.
The global() configuration object umask available in rsyslog 8.26.0+, sets the rsyslogd process' umask. If not specified, the system-provided default is used. The value given must always be a 4-digit octal number, with the initial digit being zero.
The legacy $umask parameter sets the rsyslogd process' umask. If not specified, the system-provided default is used. The value given must always be a 4-digit octal number, with the initial digit being zero.
The legacy $FileCreateMode parameter allows the setting of the mode with which rsyslogd creates new files. If not specified, the value 0644 is used. The value given must always be a 4-digit octal number, with the initial digit being zero. Please note that the actual permission depend on rsyslogd process umask If in doubt, use $umask 0000 right at the beginning of the configuration file to remove any restrictions.
The legacy $FileCreateMode may be specified multiple times. If so, it specifies the creation mode for all selector lines that follow until the next $FileCreateMode parameter. Order of lines is vitally important.
It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

### Solution

Edit either /etc/rsyslog.conf or a dedicatedconf file in /etc/rsyslog.d/ and set $FileCreateMode to 0640 or more restrictive:
$FileCreateMode 0640
Example script to create a drop-in configuration file in the default include location:
#!/usr/bin/env bash
{ [ ! -d "/etc/rsyslog.d/" ] && mkdir /etc/rsyslog.d/ printf '%s ' "" "$FileCreateMode 0640" >> /etc/rsyslog.d/60-rsyslog.conf }
Reload the service:
# systemctl reload-or-restart rsyslog

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171** | 3.3.6 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.03.01 |
| **800-171R3** | 03.03.03 |
| **800-171R3** | 03.03.06a. |

| | |
|---|---|
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | AU-2 |
| **800-53** | AU-7 |
| **800-53** | AU-12 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | AU-2 |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-12 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.3(a) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 5.1 |
| **CSCV7** | 6.2 |
| **CSCV7** | 6.3 |
| **CSCV8** | 3.3 |
| **CSCV8** | 8.2 |

|  |  |
|---|---|
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | DE.CM-7 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-1 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |

| | |
|---|---|
| **ISO-27001-2022** | A.8.15 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | AU-2 |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-12 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | M1.2.2 |
| **NESA** | M5.5.1 |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |

| | |
|---|---|
| **NIAV2** | AM3 |
| **NIAV2** | AM7 |
| **NIAV2** | AM11a |
| **NIAV2** | AM11b |
| **NIAV2** | AM11c |
| **NIAV2** | AM11d |
| **NIAV2** | AM11e |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **NIAV2** | SS30 |
| **NIAV2** | VL8 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV3.2.1** | 10.1 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **SWIFT-CSCV1** | 6.4 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

### Assets

**linux_project**

```
The command script with multiple lines returned :

- Audit Result:
```

```
** PASS **
- Parameter: "$FileCreateMode" is correctly set to mode: ""
  in the file: "/etc/rsyslog.conf"
  Should be mode: "640" or more restrictive
```

## 6.1.3.7 Ensure rsyslog is not configured to receive logs from a remote client

### Info

rsyslog supports the ability to receive messages from remote hosts, thus acting as a log server. Clients should not receive data from other hosts.
If a client is configured to also receive data, thus turning it into a server, the client system is acting outside its operational boundary.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

### Solution

Unless the system's primary function is to serve as a logfile server , modify the files returned by the Audit Procedure and remove the specific lines highlighted by the audit. Verify none of the following entries are present in the rsyslog configuration.
advanced format
module(load="imtcp") input(type="imtcp" port="514")
deprecated legacy format
$ModLoad imtcp $InputTCPServerRun
Reload the service:
# systemctl reload-or-restart rsyslog

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |

| | |
|---|---|
| **LEVEL** | 1A |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **
 - No entries to accept incoming logs found
```

## 7.1.1 Ensure permissions on /etc/passwd are configured

### Info

The /etc/passwd file contains user account information that is used by many system utilities and therefore must be readable for these utilities to operate.
It is critical to ensure that the /etc/passwd file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### Solution

Run the following commands to remove excess permissions, set owner, and set group on /etc/passwd :
# chmod u-x,go-wx /etc/passwd # chown root:root /etc/passwd

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |

| | |
|---|---|
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |

| | |
|---|---|
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |

| | |
|---|---|
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The file /etc/passwd with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/passwd
```

## 7.1.10 Ensure permissions on /etc/security/opasswd are configured

### Info

/etc/security/opasswd and it's backup /etc/security/opasswd.old hold user's previous passwords if pam_unix or pam_pwhistory is in use on the system
It is critical to ensure that /etc/security/opasswd is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### Solution

Run the following commands to remove excess permissions, set owner, and set group on /etc/security/opasswd and /etc/security/opasswd.old is they exist:

```
# [ -e "/etc/security/opasswd" ] && chmod u-x,go-rwx /etc/security/opasswd # [ -e "/etc/security/opasswd" ] && chown root:root /etc/security/opasswd # [ -e "/etc/security/opasswd.old" ] && chmod u-x,go-rwx /etc/security/opasswd.old # [ -e "/etc/security/opasswd.old" ] && chown root:root /etc/security/opasswd.old
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |

| | |
|---|---|
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |

| | |
|---|---|
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |

| | |
|---|---|
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
All of the following must pass to satisfy this requirement:

-------------------------
PASSED - etc/security/opasswd file permissions
The file /etc/security/opasswd with fmode owner: root group: root mode: 0600 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/security/opasswd

-------------------------
PASSED - /etc/security/opasswd.old file permissions
```

## 7.1.2 Ensure permissions on /etc/passwd- are configured

### Info

The /etc/passwd- file contains backup user account information.
It is critical to ensure that the /etc/passwd- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### Solution

Run the following commands to remove excess permissions, set owner, and set group on /etc/passwd- :
# chmod u-x,go-wx /etc/passwd- # chown root:root /etc/passwd-

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |

| | |
|---|---|
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |

| | |
|---|---|
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |

|  |  |
|---|---|
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

### Assets

#### linux_project

```
The file /etc/passwd- with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/passwd-
```

## 7.1.3 Ensure permissions on /etc/group are configured

### Info

The /etc/group file contains a list of all the valid groups defined in the system. The command below allows read/write access for root and read access for everyone else.
The /etc/group file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.

### Solution

Run the following commands to remove excess permissions, set owner, and set group on /etc/group :
# chmod u-x,go-wx /etc/group # chown root:root /etc/group

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |

| | |
|---|---|
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |

| | |
|---|---|
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |

|  |  |
|---|---|
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The file /etc/group with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/group
```

## 7.1.4 Ensure permissions on /etc/group- are configured

### Info

The /etc/group- file contains a backup list of all the valid groups defined in the system.
It is critical to ensure that the /etc/group- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### Solution

Run the following commands to remove excess permissions, set owner, and set group on /etc/group- :
# chmod u-x,go-wx /etc/group- # chown root:root /etc/group-

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |

| | |
|---|---|
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |

| | |
|---|---|
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |

| | |
|---|---|
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The file /etc/group- with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/group-
```

## 7.1.5 Ensure permissions on /etc/shadow are configured

### Info

The /etc/shadow file is used to store the information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.
If attackers can gain read access to the /etc/shadow file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the /etc/shadow file (such as expiration) could also be useful to subvert the user accounts.

### Solution

Run one of the following commands to set ownership of /etc/shadow to root and group to either root or shadow :
# chown root:shadow /etc/shadow
-OR- # chown root:root /etc/shadow
Run the following command to remove excess permissions form /etc/shadow :
# chmod u-x,g-wx,o-rwx /etc/shadow

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |

| | |
|---|---|
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |

| | |
|---|---|
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |

| | |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The file /etc/shadow with fmode owner: root group: shadow mode: 0640 uid: 0 gid: 42 uneven
 permissions : FALSE is compliant with the policy value

/etc/shadow
```

## 7.1.6 Ensure permissions on /etc/shadow- are configured

### Info

The /etc/shadow- file is used to store backup information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.
It is critical to ensure that the /etc/shadow- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### Solution

Run one of the following commands to set ownership of /etc/shadow- to root and group to either root or shadow :
# chown root:shadow /etc/shadow-
-OR- # chown root:root /etc/shadow-
Run the following command to remove excess permissions form /etc/shadow- :
# chmod u-x,g-wx,o-rwx /etc/shadow-

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |

| | |
|---|---|
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |

| | |
|---|---|
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |

| | |
|---|---|
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The file /etc/shadow- with fmode owner: root group: shadow mode: 0640 uid: 0 gid: 42 uneven
 permissions : FALSE is compliant with the policy value

/etc/shadow-
```

## 7.1.7 Ensure permissions on /etc/gshadow are configured

### Info

The /etc/gshadow file is used to store the information about groups that is critical to the security of those accounts, such as the hashed password and other security information.
If attackers can gain read access to the /etc/gshadow file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the /etc/gshadow file (such as group administrators) could also be useful to subvert the group.

### Solution

Run one of the following commands to set ownership of /etc/gshadow to root and group to either root or shadow :
# chown root:shadow /etc/gshadow
-OR- # chown root:root /etc/gshadow
Run the following command to remove excess permissions form /etc/gshadow :
# chmod u-x,g-wx,o-rwx /etc/gshadow

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |

| | |
|---|---|
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |

| | |
|---|---|
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |

| | |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The file /etc/gshadow with fmode owner: root group: shadow mode: 0640 uid: 0 gid: 42 uneven
 permissions : FALSE is compliant with the policy value

/etc/gshadow
```

## 7.1.8 Ensure permissions on /etc/gshadow- are configured

### Info

The /etc/gshadow- file is used to store backup information about groups that is critical to the security of those accounts, such as the hashed password and other security information.
It is critical to ensure that the /etc/gshadow- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### Solution

Run one of the following commands to set ownership of /etc/gshadow- to root and group to either root or shadow :
# chown root:shadow /etc/gshadow-
-OR- # chown root:root /etc/gshadow-
Run the following command to remove excess permissions form /etc/gshadow- :
# chmod u-x,g-wx,o-rwx /etc/gshadow-

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |

| | |
|---|---|
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |

| | |
|---|---|
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |

| | |
|---|---|
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The file /etc/gshadow- with fmode owner: root group: shadow mode: 0640 uid: 0 gid: 42 uneven
 permissions : FALSE is compliant with the policy value

/etc/gshadow-
```

## 7.1.9 Ensure permissions on /etc/shells are configured

### Info

/etc/shells is a text file which contains the full pathnames of valid login shells. This file is consulted by chsh and available to be queried by other programs.
It is critical to ensure that the /etc/shells file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### Solution

Run the following commands to remove excess permissions, set owner, and set group on /etc/shells :
# chmod u-x,go-wx /etc/shells # chown root:root /etc/shells

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |

| | |
|---|---|
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |

| | |
|---|---|
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |

|  |  |
|---|---|
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The file /etc/shells with fmode owner: root group: root mode: 0644 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/shells
```

## 7.2.1 Ensure accounts in /etc/passwd use shadowed passwords

### Info

Local accounts can uses shadowed passwords. With shadowed passwords, The passwords are saved in shadow password file, /etc/shadow encrypted by a salted one-way hash. Accounts with a shadowed password have an x in the second field in /etc/passwd
The /etc/passwd file also contains information like user ID's and group ID's that are used by many system programs. Therefore, the /etc/passwd file must remain world readable. In spite of encoding the password with a randomly-generated one-way hash function, an attacker could still break the system if they got access to the /etc/passwd file. This can be mitigated by using shadowed passwords, thus moving the passwords in the /etc/passwd file to /etc/shadow The /etc/shadow file is set so only root will be able to read and write. This helps mitigate the risk of an attacker gaining access to the encoded passwords with which to perform a dictionary attack.
Note:
- All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.
- A user account with an empty second field in /etc/passwd allows the account to be logged into by providing only the username.

### Solution

Run the following command to set accounts to use shadowed passwords and migrate passwords in /etc/passwd to /etc/shadow :

```
# pwconv
```

Investigate to determine if the account is logged in and what it is being used for, to determine if it needs to be forced off.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171** | 3.13.16 |
| **800-171R3** | 03.05.07 |
| **800-171R3** | 03.13.08 |
| **800-53** | IA-5(1) |
| **800-53** | SC-28 |
| **800-53** | SC-28(1) |
| **800-53R5** | IA-5(1) |
| **800-53R5** | SC-28 |
| **800-53R5** | SC-28(1) |
| **CN-L3** | 8.1.4.7(b) |
| **CN-L3** | 8.1.4.8(b) |
| **CSCV7** | 16.4 |
| **CSCV8** | 3.11 |
| **CSF** | PR.AC-1 |
| **CSF** | PR.DS-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |

| | |
|---|---|
| **CSF2.0** | PR.DS-01 |
| **GDPR** | 32.1.a |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(a)(2)(iv) |
| **HIPAA** | 164.312(d) |
| **HIPAA** | 164.312(e)(2)(ii) |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ISO-27001-2022** | A.5.33 |
| **ITSG-33** | IA-5(1) |
| **ITSG-33** | SC-28 |
| **ITSG-33** | SC-28a. |
| **ITSG-33** | SC-28(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **PCI-DSSV3.2.1** | 3.4 |
| **PCI-DSSV4.0** | 3.3.2 |
| **PCI-DSSV4.0** | 3.5.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |
| **TBA-FIISB** | 28.1 |

## Assets

### linux_project

```
The command '/bin/awk -F: '($2 != "x" ) { print $1 " is not set to shadowed passwords "}' /etc/
passwd | /bin/awk '{print} END {if (NR == 0) print "none"}'' returned :

none
```

## 7.2.10 Ensure local interactive user dot files access is configured

### Info

While the system administrator can establish secure permissions for users' "dot" files, the users can easily override these.
- forward file specifies an email address to forward the user's mail to.
- rhost file provides the "remote authentication" database for the rcp, rlogin, and rsh commands and the rcmd() function. These files bypass the standard password-based user authentication mechanism. They specify remote hosts and users that are considered trusted (i.e. are allowed to access the local system without supplying a password)
- netrc file contains data for logging into a remote host or passing authentication to an API.
- bash_history file keeps track of the user's commands.
User configuration files with excessive or incorrect access may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

### Solution

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user dot file permissions and determine the action to be taken in accordance with site policy.
The following script will:
- remove excessive permissions on dot files within interactive users' home directories
- change ownership of dot files within interactive users' home directories to the user
- change group ownership of dot files within interactive users' home directories to the user's primary group
- listforward andrhost files to be investigated and manually deleted

```
#!/usr/bin/env bash
{ a_output2=(); a_output3=() l_maxsize="1000" # Maximum number of local interactive users before warning (Default
1,000) l_valid_shells="^($( awk -F/ '$NF != "nologin" {print}' /etc/shells | sed -rn '/^\//{s,/,\\/,g;p}' | paste -s -d '|' - ))$"
a_user_and_home=() # Create array with local users and their home directories while read -r l_local_user
l_local_user_home; do # Populate array with users and user home location [[ -n "$l_local_user" && -n
"$l_local_user_home" ]] && a_user_and_home+=("$l_local_user:$l_local_user_home") done <<< "$(awk -v
pat="$l_valid_shells" -F: '$(NF) ~ pat { print $1 " " $(NF-1) }' /etc/passwd)"
l_asize="${#a_user_and_home[@]}" # Here if we want to look at number of users before proceeding
[ "${#a_user_and_home[@]}" -gt "$l_maxsize" ] && printf '%s ' "" " ** INFO **" " - \"$l_asize\" Local interactive users
found on the system" " - This may be a long running check" ""
file_access_fix() { a_access_out=() l_max="$( printf '%o' $(( 0777 & ~$l_mask)) )"
if [ $(( $l_mode & $l_mask )) -gt 0 ]; then printf '%s ' "" " - File: \"$l_hdfile\" is mode: \"$l_mode\" and should be mode:
\"$l_max\" or more restrictive" " Updating file: \"$l_hdfile\" to be mode: \"$l_max\" or more restrictive"
chmod "$l_change" "$l_hdfile"
fi if [[ ! "$l_owner" =~ ($l_user) ]]; then printf '%s ' "" " - File: \"$l_hdfile\" owned by: \"$l_owner\" and should be owned
by \"${l_user//|/ or }\"" " Updating file: \"$l_hdfile\" to be owned by \"${l_user//|/ or }\""
chown "$l_user" "$l_hdfile"
fi if [[ ! "$l_gowner" =~ ($l_group) ]]; then printf '%s ' "" " - File: \"$l_hdfile\" group owned by: \"$l_gowner\" and should
be group owned by \"${l_group//|/ or }\"" " Updating file: \"$l_hdfile\" to be group owned by \"${l_group//|/ or }\""
chgrp "$l_group" "$l_hdfile"
fi } while IFS=: read -r l_user l_home; do a_dot_file=(); a_netrc=(); a_netrc_warn=(); a_bhout=(); a_hdirout=() if [ -d
"$l_home" ]; then l_group="$(id -gn "$l_user" | xargs)";l_group="${l_group// /|}"
while IFS= read -r -d $'0' l_hdfile; do while read -r l_mode l_owner l_gowner; do case "$(basename "$l_hdfile")"
in .forward | .rhost ) a_dot_file+=(" - File: \"$l_hdfile\" exists" " Please review and manually delete this file") ;;
.netrc ) l_mask='0177'; l_change="u-x,go-rwx"; file_access_fix a_netrc_warn+=(" - File: \"$l_hdfile\" exists") ;;
.bash_history ) l_mask='0177'; l_change="u-x,go-rwx"; file_access_fix ;;
* ) l_mask='0133'; l_change="u-x,go-wx"; file_access_fix ;;
esac done < <(stat -Lc '%#a %U %G' "$l_hdfile") done < <(find "$l_home" -xdev -type f -name '.*' -
print0) fi [ "${#a_dot_file[@]}" -gt 0 ] && a_output2+=(" - User: \"$l_user\" Home Directory: \"$l_home\""
"${a_dot_file[@]}") [ "${#a_netrc_warn[@]}" -gt 0 ] && a_output3+=(" - User: \"$l_user\" Home Directory: \"$l_home\""
"${a_netrc_warn[@]}") done <<< "$(printf '%s ' "${a_user_and_home[@]}")"
[ "${#a_output3[@]}" -gt 0 ] && printf '%s ' "" " ** WARNING **" "${a_output3[@]}" ""
[ "${#a_output2[@]}" -gt 0 ] && printf '%s ' "" "${a_output2[@]}"
}
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |

| | |
|---|---|
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |

| | |
|---|---|
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |

| | |
|---|---|
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **
 - * Correctly configured * :
  - No local interactive users home directories contain:
   - ".forward" or ".rhost" files
   - ".netrc" files with incorrect access configured
   - ".bash_history" files with incorrect access configured
   - "dot" files with incorrect access configured
```

## 7.2.2 Ensure /etc/shadow password fields are not empty

### Info

An account with an empty password field means that anybody may log in as that user without providing a password. All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.

### Solution

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it can be determined why it does not have a password:
# passwd -l <username>
Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be forced off.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.2 |
| **800-171R3** | 03.05.07 |
| **800-53** | IA-5(1) |
| **800-53R5** | IA-5(1) |
| **CSCV7** | 4.4 |
| **CSCV8** | 5.2 |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ITSG-33** | IA-5(1) |
| **LEVEL** | 1A |
| **NESA** | T5.2.3 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 4.1 |

### Assets

#### linux_project

```
The command '/bin/awk -F : '($2 == "") { print $1 " does not have a password."}' /etc/shadow | /
bin/awk '{print} END {if (NR == 0) print "none"}'' returned :
```

none

## 7.2.3 Ensure all groups in /etc/passwd exist in /etc/group

### Info

Over time, system administration errors and changes can lead to groups being defined in /etc/passwd but not in /etc/group
Groups defined in the /etc/passwd file but not in the /etc/group file pose a threat to system security since group permissions are not properly managed.

### Solution

Analyze the output of the Audit step above and perform the appropriate action to correct any discrepancies found.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.01 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-2 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | AT-2 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(d) |
| **CN-L3** | 7.1.3.2(g) |

| | |
|---|---|
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV8** | 3.3 |
| **CSCV8** | 14.6 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |
| **CSF** | PR.AC-1 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.18 |
| **ISO-27001-2022** | A.5.33 |

| | |
|---|---|
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.2.1 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-2 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |

| | |
|---|---|
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | AM28 |
| **NIAV2** | NS5j |
| **NIAV2** | SS13c |
| **NIAV2** | SS14e |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 13.2 |
| **QCSC-V1** | 15.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
No issues found.
```

## 7.2.4 Ensure shadow group is empty

### Info

The shadow group allows system programs which require access the ability to read the /etc/shadow file. No users should be assigned to the shadow group.

Any users assigned to the shadow group would be granted read access to the /etc/shadow file. If attackers can gain read access to the /etc/shadow file, they can easily run a password cracking program against the hashed passwords to break them. Other security information that is stored in the /etc/shadow file (such as expiration) could also be useful to subvert additional user accounts.

### Solution

Run the following command to remove all users from the shadow group

```
# sed -ri 's/(^shadow:[^:]*:[^:]*:)([^:]+$)/1/' /etc/group
```

Change the primary group of any users with shadow as their primary group.

```
# usermod -g <primary group> <user>
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |

| | |
|---|---|
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |

| | |
|---|---|
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |

| | |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The command '/bin/awk -F: 'FILENAME == "/etc/group" && $1 == "shadow" { gid=$3; if ($4!="")
 { print "secondary "$4; f=1 } } FILENAME == "/etc/passwd" && $4 == gid { print "primary "$1;
 f=1 } END { if (!f) print "shadow group empty" }' /etc/group /etc/passwd' returned :

shadow group empty
```

## 7.2.5 Ensure no duplicate UIDs exist

### Info

Although the useradd program will not let you create a duplicate User ID (UID), it is possible for an administrator to manually edit the /etc/passwd file and change the UID field.
Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.

### Solution

Based on the results of the audit script, establish unique UIDs and review all files owned by the shared UIDs to determine which UID they are supposed to belong to.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.5 |
| **800-171** | 3.5.6 |
| **800-171R3** | 03.05.05c. |
| **800-53** | IA-4d. |
| **800-53R5** | IA-4d. |
| **CN-L3** | 8.1.4.1(a) |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ITSG-33** | IA-4d. |
| **LEVEL** | 1A |
| **NESA** | T5.5.2 |
| **NIAV2** | AM14a |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5 |

### Assets

#### linux_project

```
No duplicate User IDs detected
```

## 7.2.6 Ensure no duplicate GIDs exist

### Info

Although the groupadd program will not let you create a duplicate Group ID (GID), it is possible for an administrator to manually edit the /etc/group file and change the GID field.
User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.

### Solution

Based on the results of the audit script, establish unique GIDs and review all files owned by the shared GID to determine which group they are supposed to belong to.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.5 |
| **800-171** | 3.5.6 |
| **800-171R3** | 03.05.05c. |
| **800-53** | IA-4d. |
| **800-53R5** | IA-4d. |
| **CN-L3** | 8.1.4.1(a) |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ITSG-33** | IA-4d. |
| **LEVEL** | 1A |
| **NESA** | T5.5.2 |
| **NIAV2** | AM14a |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5 |

### Assets

**linux_project**

```
No duplicate Group IDs detected
```

## 7.2.7 Ensure no duplicate user names exist

### Info

Although the useradd program will not let you create a duplicate user name, it is possible for an administrator to manually edit the /etc/passwd file and change the user name.
If a user is assigned a duplicate user name, it will create and have access to files with the first UID for that username in /etc/passwd For example, if "test4" has a UID of 1000 and a subsequent "test4" entry has a UID of 2000, logging in as "test4" will use UID 1000. Effectively, the UID is shared, which is a security problem.

### Solution

Based on the results of the audit script, establish unique user names for the users. File ownerships will automatically reflect the change as long as the users have unique UIDs.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.5 |
| **800-171** | 3.5.6 |
| **800-171R3** | 03.05.05c. |
| **800-53** | IA-4d. |
| **800-53R5** | IA-4d. |
| **CN-L3** | 8.1.4.1(a) |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ITSG-33** | IA-4d. |
| **LEVEL** | 1A |
| **NESA** | T5.5.2 |
| **NIAV2** | AM14a |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5 |

### Assets

**linux_project**

```
No issues found.
```

## 7.2.8 Ensure no duplicate group names exist

### Info

Although the groupadd program will not let you create a duplicate group name, it is possible for an administrator to manually edit the /etc/group file and change the group name.
If a group is assigned a duplicate group name, it will create and have access to files with the first GID for that group in /etc/group Effectively, the GID is shared, which is a security problem.

### Solution

Based on the results of the audit script, establish unique names for the user groups. File group ownerships will automatically reflect the change as long as the groups have unique GIDs.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.5.5 |
| **800-171** | 3.5.6 |
| **800-171R3** | 03.05.05c. |
| **800-53** | IA-4d. |
| **800-53R5** | IA-4d. |
| **CN-L3** | 8.1.4.1(a) |
| **CSF** | PR.AC-1 |
| **CSF2.0** | PR.AA-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |
| **ISO-27001-2022** | A.5.16 |
| **ITSG-33** | IA-4d. |
| **LEVEL** | 1A |
| **NESA** | T5.5.2 |
| **NIAV2** | AM14a |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5 |

### Assets

#### linux_project

```
No issues found.
```

## 7.2.9 Ensure local interactive user home directories are configured

### Info

The user home directory is space defined for the particular user to set local environment variables and to store personal files. While the system administrator can establish secure permissions for users' home directories, the users can easily override these. Users can be defined in /etc/passwd without a home directory or with a home directory that does not actually exist.
Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory. Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges. If the user's home directory does not exist or is unassigned, the user will be placed in "/" and will not be able to write any files or have local environment variables set.

### Solution

If a local interactive users' home directory is undefined and/or doesn't exist, follow local site policy and perform one of the following:
- Lock the user account
- Remove the user from the system
- create a directory for the user. If undefined, edit /etc/passwd and add the absolute path to the directory to the last field of the user.

Run the following script to:
- Remove excessive permissions from local interactive users home directories
- Update the home directory's owner

```
#!/usr/bin/env bash
{ l_output2=""
l_valid_shells="^($( awk -F/ '$NF != "nologin" {print}' /etc/shells | sed -rn '/^//{s,/,\\/,g;p}' | paste -s -d '|' - ))$"
unset a_uarr && a_uarr=() # Clear and initialize array while read -r l_epu l_eph; do # Populate array with users and user home location a_uarr+=("$l_epu $l_eph") done <<< "$(awk -v pat="$l_valid_shells" -F: '$(NF) ~ pat { print $1 " " $(NF-1) }' /etc/passwd)"
l_asize="${#a_uarr[@]}" # Here if we want to look at number of users before proceeding [ "$l_asize " -gt "10000" ] && echo -e "
** INFO **
- \"$l_asize\" Local interactive users found on the system
- This may be a long running process "
while read -r l_user l_home; do if [ -d "$l_home" ]; then l_mask='0027'
l_max="$( printf '%o' $(( 0777 & ~$l_mask)) )"
while read -r l_own l_mode; do if [ "$l_user" != "$l_own" ]; then l_output2="$l_output2
- User: \"$l_user\" Home \"$l_home\" is owned by: \"$l_own\"
- changing ownership to: \"$l_user\"
"
chown "$l_user" "$l_home"
fi if [ $(( $l_mode & $l_mask )) -gt 0 ]; then l_output2="$l_output2
- User: \"$l_user\" Home \"$l_home\" is mode: \"$l_mode\" should be mode: \"$l_max\" or more restrictive
- removing excess permissions "
chmod g-w,o-rwx "$l_home"
fi done <<< "$(stat -Lc '%U %#a' "$l_home")"
else l_output2="$l_output2
- User: \"$l_user\" Home \"$l_home\" Doesn't exist
- Please create a home in accordance with local site policy"
fi done <<< "$(printf '%s ' "${a_uarr[@]}")"
if [ -z "$l_output2" ]; then # If l_output2 is empty, we pass echo -e " - No modification needed to local interactive users home directories"
else echo -e "
$l_output2"
fi }
```

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |

| | |
|---|---|
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |

| | |
|---|---|
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1A |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |

|  |  |
|---|---|
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **
 - * Correctly configured * :
  - All local interactive users:
   - home directories exist
   - own their home directory
   - home directories are mode: "750" or more restrictive
```

### CIS_Ubuntu_Linux_24.04_LTS_v1.0.0_L1_Server.audit from CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0

#### Info

#### Solution

#### See Also

https://workbench.cisecurity.org/benchmarks/18959

#### Assets

**linux_project**

# Audits INFO,WARNING,ERROR

## 1.1.1.10 Ensure unused filesystems kernel modules are not available

### Info

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

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

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

- afs - CVE-2022-37402
- ceph - CVE-2022-0670
- cifs - CVE-2022-29869
- exfat CVE-2022-29973
- ext CVE-2022-1184
- fat CVE-2022-22043
- fscache CVE-2022-3630
- fuse CVE-2023-0386
- gfs2 CVE-2023-3212
- nfs_common CVE-2023-6660
- nfsd CVE-2022-43945
- smbfs_common CVE-2022-2585

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

### Solution

- IF - the module is available in the running kernel:
- Unload the filesystem kernel module from the kernel
- Create a file ending inconf with install filesystem kernel modules /bin/false in the /etc/modprobe.d/ directory
- Create a file ending inconf with deny list filesystem kernel modules in the /etc/modprobe.d/ directory

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

Example of unloading the gfs2 kernel module:

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

Example of fully disabling the gfs2 kernel module:

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

Note:

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

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

Example Script

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

Impact:

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

## See Also

https://workbench.cisecurity.org/benchmarks/18959

## References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1M |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command script with multiple lines returned :

-- INFO --
The following intentionally skipped
 - Kernel module: "xfs"
```

```
-- Audit Result: --
  ** REVIEW the following **
  - Kernel module: "autofs" is not fully disabled
  - Kernel module: "ufs" is not fully disabled
  - Kernel module: "dlm" is not fully disabled
  - Kernel module: "isofs" is not fully disabled
  - Kernel module: "9p" is not fully disabled
  - Kernel module: "nfs_common" is not fully disabled  <- CVE exists!
  - Kernel module: "smb" is not fully disabled
  - Kernel module: "netfs" is not fully disabled
  - Kernel module: "cachefiles" is not fully disabled
  - Kernel module: "btrfs" is not fully disabled
  - Kernel module: "nls" is not fully disabled
  - Kernel module: "fat" is not fully disabled  <- CVE exists!
  - Kernel module: "nfsd" is not fully disabled  <- CVE exists!
  - Kernel module: "lockd" is not fully disabled
  - Kernel module: "fuse" is not fully disabled  <- CVE exists!
  - Kernel module: "ceph" is not fully disabled  <- CVE exists!
  - Kernel module: "nfs" is not fully disabled
  - Kernel module: "overlay" is not fully disabled
  - Kernel module: "vboxsf" is not fully disabled
  - Kernel module: "udf" is not fully disabled
  - Kernel module: "erofs" is not fully disabled
```

## 1.2.1.1 Ensure GPG keys are configured

### Info

Most package managers implement GPG key signing to verify package integrity during installation.
It is important to ensure that updates are obtained from a valid source to protect against spoofing that could lead to the inadvertent installation of malware on the system.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

### Solution

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

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.11.2 |
| **800-171** | 3.11.3 |
| **800-171** | 3.14.1 |
| **800-171R3** | 03.11.02 |
| **800-171R3** | 03.14.01 |
| **800-53** | RA-5 |
| **800-53** | SI-2 |
| **800-53** | SI-2(2) |
| **800-53R5** | RA-5 |
| **800-53R5** | RA-7 |
| **800-53R5** | SI-2 |
| **800-53R5** | SI-2(2) |
| **CN-L3** | 8.1.4.4(e) |
| **CN-L3** | 8.1.10.5(a) |
| **CN-L3** | 8.1.10.5(b) |
| **CN-L3** | 8.5.4.1(b) |
| **CN-L3** | 8.5.4.1(d) |
| **CN-L3** | 8.5.4.1(e) |
| **CSCV7** | 3.4 |
| **CSCV7** | 3.5 |
| **CSCV8** | 7.3 |
| **CSCV8** | 7.4 |
| **CSF** | DE.CM-8 |
| **CSF** | DE.DP-4 |

| | |
|---|---|
| **CSF** | DE.DP-5 |
| **CSF** | ID.RA-1 |
| **CSF** | PR.IP-12 |
| **CSF** | RS.CO-3 |
| **CSF** | RS.MI-3 |
| **CSF2.0** | GV.SC-10 |
| **CSF2.0** | ID.IM-01 |
| **CSF2.0** | ID.IM-02 |
| **CSF2.0** | ID.IM-03 |
| **CSF2.0** | ID.RA-01 |
| **CSF2.0** | ID.RA-08 |
| **CSF2.0** | PR.PS-02 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.6.8 |
| **ISO-27001-2022** | A.8.8 |
| **ISO-27001-2022** | A.8.32 |
| **ISO/IEC-27001** | A.12.6.1 |
| **ITSG-33** | RA-5 |
| **ITSG-33** | SI-2 |
| **ITSG-33** | SI-2(2) |
| **LEVEL** | 1M |
| **NESA** | M1.2.2 |
| **NESA** | M5.4.1 |
| **NESA** | T7.6.2 |
| **NESA** | T7.7.1 |
| **NIAV2** | PR9 |
| **PCI-DSSV3.2.1** | 6.1 |
| **PCI-DSSV3.2.1** | 6.2 |
| **PCI-DSSV4.0** | 6.3 |

| | |
|---|---|
| **PCI-DSSV4.0** | 6.3.1 |
| **PCI-DSSV4.0** | 6.3.3 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **SWIFT-CSCV1** | 2.2 |
| **SWIFT-CSCV1** | 2.7 |

## Assets

### linux_project

```
The command '/bin/apt-key list' returned :

Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
/etc/apt/trusted.gpg.d/monarx.asc
---------------------------------
pub   rsa4096 2017-11-17 [SC]
      CF08 CC77 8AF9 ADDD 41AE  2D44 4E24 0071 0231 38C8
uid           [ unknown] Monarx Admin <admin@monarx.com>
sub   rsa4096 2017-11-17 [E]

/etc/apt/trusted.gpg.d/ubuntu-keyring-2012-cdimage.gpg
------------------------------------------------------
pub   rsa4096 2012-05-11 [SC]
      8439 38DF 228D 22F7 B374  2BC0 D94A A3F0 EFE2 1092
uid           [ unknown] Ubuntu CD Image Automatic Signing Key (2012) <cdimage@ubuntu.com>

/etc/apt/trusted.gpg.d/ubuntu-keyring-2018-archive.gpg
------------------------------------------------------
pub   rsa4096 2018-09-17 [SC]
      F6EC B376 2474 EDA9 D21B  7022 8719 20D1 991B C93C
uid           [ unknown] Ubuntu Archive Automatic Signing Key (2018) <ftpmaster@ubuntu.com>
```

## 1.2.1.2 Ensure package manager repositories are configured

### Info

Systems need to have package manager repositories configured to ensure they receive the latest patches and updates.

If a system's package repositories are misconfigured important patches may not be identified or a rogue repository could introduce compromised software.

NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

### Solution

Configure your package manager repositories according to site policy.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.11.2 |
| **800-171** | 3.11.3 |
| **800-171** | 3.14.1 |
| **800-171R3** | 03.11.02 |
| **800-171R3** | 03.14.01 |
| **800-53** | RA-5 |
| **800-53** | SI-2 |
| **800-53** | SI-2(2) |
| **800-53R5** | RA-5 |
| **800-53R5** | RA-7 |
| **800-53R5** | SI-2 |
| **800-53R5** | SI-2(2) |
| **CN-L3** | 8.1.4.4(e) |
| **CN-L3** | 8.1.10.5(a) |
| **CN-L3** | 8.1.10.5(b) |
| **CN-L3** | 8.5.4.1(b) |
| **CN-L3** | 8.5.4.1(d) |
| **CN-L3** | 8.5.4.1(e) |
| **CSCV7** | 3.4 |
| **CSCV7** | 3.5 |
| **CSCV8** | 7.3 |
| **CSCV8** | 7.4 |
| **CSF** | DE.CM-8 |

| | |
|---|---|
| **CSF** | DE.DP-4 |
| **CSF** | DE.DP-5 |
| **CSF** | ID.RA-1 |
| **CSF** | PR.IP-12 |
| **CSF** | RS.CO-3 |
| **CSF** | RS.MI-3 |
| **CSF2.0** | GV.SC-10 |
| **CSF2.0** | ID.IM-01 |
| **CSF2.0** | ID.IM-02 |
| **CSF2.0** | ID.IM-03 |
| **CSF2.0** | ID.RA-01 |
| **CSF2.0** | ID.RA-08 |
| **CSF2.0** | PR.PS-02 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.6.8 |
| **ISO-27001-2022** | A.8.8 |
| **ISO-27001-2022** | A.8.32 |
| **ISO/IEC-27001** | A.12.6.1 |
| **ITSG-33** | RA-5 |
| **ITSG-33** | SI-2 |
| **ITSG-33** | SI-2(2) |
| **LEVEL** | 1M |
| **NESA** | M1.2.2 |
| **NESA** | M5.4.1 |
| **NESA** | T7.6.2 |
| **NESA** | T7.7.1 |
| **NIAV2** | PR9 |
| **PCI-DSSV3.2.1** | 6.1 |
| **PCI-DSSV3.2.1** | 6.2 |

| | |
|---|---|
| **PCI-DSSV4.0** | 6.3 |
| **PCI-DSSV4.0** | 6.3.1 |
| **PCI-DSSV4.0** | 6.3.3 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **SWIFT-CSCV1** | 2.2 |
| **SWIFT-CSCV1** | 2.7 |

## Assets

### linux_project

```
 The command '/bin/apt-cache policy' returned :

Package files:
 100 /var/lib/dpkg/status
     release a=now
 500 http://us.archive.ubuntu.com/ubuntu noble-security/multiverse amd64 Packages
     release v=24.04,o=Ubuntu,a=noble-security,n=noble,l=Ubuntu,c=multiverse,b=amd64
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu noble-security/restricted amd64 Packages
     release v=24.04,o=Ubuntu,a=noble-security,n=noble,l=Ubuntu,c=restricted,b=amd64
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu noble-security/universe amd64 Packages
     release v=24.04,o=Ubuntu,a=noble-security,n=noble,l=Ubuntu,c=universe,b=amd64
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu noble-security/main amd64 Packages
     release v=24.04,o=Ubuntu,a=noble-security,n=noble,l=Ubuntu,c=main,b=amd64
     origin us.archive.ubuntu.com
 100 http://us.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Packages
     release v=24.04,o=Ubuntu,a=noble-backports,n=noble,l=Ubuntu,c=universe,b=amd64
     origin us.archive.ubuntu.com
 100 http://us.archive.ubuntu.com/ubuntu noble-backports/main amd64 Packages
     release v=24.04,o=Ubuntu,a=noble-backports,n=noble,l=Ubuntu,c=main,b=amd64
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages
     release v=24.04,o=Ubuntu,a=noble-updates,n=noble,l=Ubuntu,c=multiverse,b=amd64
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages
     release v=24.04,o=Ubuntu,a=noble-updates,n=noble,l=Ubuntu,c=restricted,b=amd64
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages
     release v=24.04,o=Ubuntu,a=noble-updates,n=noble,l=Ubuntu,c=universe,b=amd64
     origin us.archive.ubuntu.com
 500 http://us.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages
     release v=24.04,o=Ubuntu,a=noble-updates,n=noble,l=Ubuntu,c=main,b=amd64
    [...]
```

## 2.1.22 Ensure only approved services are listening on a network interface

### Info

A network port is identified by its number, the associated IP address, and the type of the communication protocol such as TCP or UDP.
A listening port is a network port on which an application or process listens on, acting as a communication endpoint.
Each listening port can be open or closed (filtered) using a firewall. In general terms, an open port is a network port that accepts incoming packets from remote locations.
Services listening on the system pose a potential risk as an attack vector. These services should be reviewed, and if not required, the service should be stopped, and the package containing the service should be removed. If required packages have a dependency, the service should be stopped and masked to reduce the attack surface of the system.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

### Solution

Run the following commands to stop the service and remove the package containing the service:
# systemctl stop <service_name>.socket <service_name>.service # apt purge <package_name>
- OR - If required packages have a dependency:
Run the following commands to stop and mask the service and socket:
# systemctl stop <service_name>.socket <service_name>.service # systemctl mask <service_name>.socket <service_name>.service
Note: replace <service_name> with the appropriate service name.
Impact:
There may be packages that are dependent on the service's package. If the service's package is removed, these dependent packages will be removed as well. Before removing the service's package, review any dependent packages to determine if they are required on the system.
- IF - a dependent package is required: stop and mask the <service_name>.socket and <service_name>.service leaving the service's package installed.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |

|  |  |
|---|---|
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1M |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
 The command '/bin/ss -plntu' returned :

Netid State  Recv-Q Send-Q Local Address:Port  Peer Address:PortProcess

udp   UNCONN 0      0         127.0.0.54:53         0.0.0.0:*    users:(("systemd-
resolve",pid=692,fd=16))
udp   UNCONN 0      0      127.0.0.53%lo:53         0.0.0.0:*    users:(("systemd-
resolve",pid=692,fd=14))
udp   UNCONN 0      0            0.0.0.0:443        0.0.0.0:*    users:(("docker-
proxy",pid=2419,fd=7))
udp   UNCONN 0      0            0.0.0.0:1194       0.0.0.0:*    users:(("openvpn",pid=2098,fd=5))

udp   UNCONN 0      0          127.0.0.1:1721       0.0.0.0:*    users:(("monarx-
agent",pid=812,fd=13))
udp   UNCONN 0      0            0.0.0.0:4789       0.0.0.0:*

udp   UNCONN 0      0               [::]:443           [::]:*    users:(("docker-
proxy",pid=2426,fd=7))
udp   UNCONN 0      0                  *:7946             *:*    users:
(("dockerd",pid=1020,fd=33))
tcp   LISTEN 0      4096       127.0.0.1:65529      0.0.0.0:*    users:(("monarx-
agent",pid=812,fd=10))
tcp   LISTEN 0      4096      127.0.0.54:53         0.0.0.0:*    users:(("systemd-
resolve",pid=692,fd=17))
tcp   LISTEN 0      4096         0.0.0.0:80         0.0.0.0:*    users:(("docker-
proxy",pid=2390,fd=7))
tcp   LISTEN 0      4096         0.0.0.0:443        0.0.0.0:*    users:(("docker-
proxy",pid=2404,fd=7))
tcp   LISTEN 0      70           0.0.0.0:33060      0.0.0.0:*    users:(("mysqld",pid=1021,fd=21))

tcp   LISTEN 0      4096         0.0.0.0:3000       0.0.0.0:*    users:(("docker-
proxy",pid=3038,fd=7))
tcp   LISTEN 0      [...]
```

## 3.1.1 Ensure IPv6 status is identified

### Info

Internet Protocol Version 6 (IPv6) is the most recent version of Internet Protocol (IP). It's designed to supply IP addressing and additional security to support the predicted growth of connected devices. IPv6 is based on 128-bit addressing and can support 340 undecillion, which is 340,282,366,920,938,463,463,374,607,431,768,211,456 unique addresses.
Features of IPv6
- Hierarchical addressing and routing infrastructure
- Statefull and Stateless configuration
- Support for quality of service (QoS)
- An ideal protocol for neighboring node interaction

IETF RFC 4038 recommends that applications are built with an assumption of dual stack. It is recommended that IPv6 be enabled and configured in accordance with Benchmark recommendations.
- IF - dual stack and IPv6 are not used in your environment, IPv6 may be disabled to reduce the attack surface of the system, and recommendations pertaining to IPv6 can be skipped.

Note: It is recommended that IPv6 be enabled and configured unless this is against local site policy
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

### Solution

Enable or disable IPv6 in accordance with system requirements and local site policy
Impact:
IETF RFC 4038 recommends that applications are built with an assumption of dual stack.
When enabled, IPv6 will require additional configuration to reduce risk to the system.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.4.2 |
| **800-171** | 3.4.6 |
| **800-171** | 3.4.7 |
| **800-171R3** | 03.04.02 |
| **800-171R3** | 03.04.06 |
| **800-53** | CM-6 |
| **800-53** | CM-7 |
| **800-53R5** | CM-6 |
| **800-53R5** | CM-7 |
| **CSCV7** | 9.2 |
| **CSCV8** | 4.8 |
| **CSF** | PR.IP-1 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |

|  |  |
|---|---|
| **ISO-27001-2022** | A.8.9 |
| **ITSG-33** | CM-6 |
| **ITSG-33** | CM-7 |
| **LEVEL** | 1M |
| **NIAV2** | SS15a |
| **PCI-DSSV3.2.1** | 2.2.2 |
| **SWIFT-CSCV1** | 2.3 |

## Assets

### linux_project

```
The command '/bin/grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && echo -e "\n - IPv6 is
 enabled\n" || echo -e "\n - IPv6 is not enabled\n"' returned :

-e
 - IPv6 is enabled
```

## 4.4.2.3 Ensure iptables outbound and established connections are configured

### Info

Configure the firewall rules for new outbound, and established connections.
Note:
- Changing firewall settings while connected over network can result in being locked out of the system
- Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well
If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

### Solution

Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:
# iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT # iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT # iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT # iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |

| | |
|---|---|
| **CSF** | PR.PT-4 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1M |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |

| | |
|---|---|
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

## Assets

### linux_project

```
 The command '/sbin/iptables -L -v -n' returned :

# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain INPUT (policy ACCEPT 14M packets, 2011M bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy DROP 4 packets, 208 bytes)
 pkts bytes target     prot opt in     out     source               destination
  15M 3137M DOCKER-USER  0    --  *      *       0.0.0.0/0            0.0.0.0/0
  15M 3137M DOCKER-FORWARD  0    --  *      *       0.0.0.0/0            0.0.0.0/0
  11M  500M ACCEPT     0    --  *      *       192.168.255.0/24     0.0.0.0/0
 808K 2343M ACCEPT     0    --  *      *       0.0.0.0/0            192.168.255.0/24

Chain OUTPUT (policy ACCEPT 5034K packets, 2881M bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain DOCKER (2 references)
 pkts bytes target     prot opt in     out     source               destination
 158K 9426K ACCEPT     6    --  !docker_gwbridge docker_gwbridge  0.0.0.0/0            172.18.0.9
          tcp dpt:3000
   25 22093 ACCEPT     17   --  !docker_gwbridge docker_gwbridge  0.0.0.0/0            172.18.0.3
          udp dpt:443
 113K 5909K ACCEPT     6    --  !docker_gwbridge docker_gwbridge  0.0.0.0/0            172.18.0.3
          tcp dpt:443
 7777  458K ACCEPT     6    --  !docker_gwbridge docker_gwbridge  0.0.0.0/0            172.18.0.3
          tcp dpt:80
    0     0 DROP       0    --  !docker_gwbridge docker_gwbridge  0.0.0.0/0            0.0.0.0/0

    0     0 DROP       0    --  !docker0 docker0  0.0.0.0/0            0.0.0.0/0

Chain DOCKER-BRIDGE (1 references)
 pkts bytes target     prot opt in     out     source               destination
 279K   16M DOCKER     0    --  *      docker_gwbridge  0.0.0.0/0            0.0.0.0/0
    0     0 DOCKER     0    --  *      docker0  0.0.0.0/0            0.0.0.0/0

Chain [...]
```

## 4.4.2.4 Ensure iptables firewall rules exist for all open ports

### Info

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.
Notes:
- Changing firewall settings while connected over network can result in being locked out of the system
- Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well
- The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy
Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

### Solution

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:
# iptables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j ACCEPT

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |

| | |
|---|---|
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1A |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |
| **QCSC-V1** | 5.2.1 |

| | |
|---|---|
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

## Assets

### linux_project

```
The command '/bin/ss -4tuln; /sbin/iptables -L INPUT -v -n' returned :

# Warning: iptables-legacy tables present, use iptables-legacy to see them
Netid State  Recv-Q Send-Q Local Address:Port  Peer Address:PortProcess
udp   UNCONN 0      0         127.0.0.54:53         0.0.0.0:*
udp   UNCONN 0      0      127.0.0.53%lo:53         0.0.0.0:*
udp   UNCONN 0      0            0.0.0.0:443        0.0.0.0:*
udp   UNCONN 0      0            0.0.0.0:1194       0.0.0.0:*
udp   UNCONN 0      0          127.0.0.1:1721       0.0.0.0:*
udp   UNCONN 0      0            0.0.0.0:4789       0.0.0.0:*
tcp   LISTEN 0      4096       127.0.0.1:65529      0.0.0.0:*
tcp   LISTEN 0      4096      127.0.0.54:53         0.0.0.0:*
tcp   LISTEN 0      4096         0.0.0.0:80         0.0.0.0:*
tcp   LISTEN 0      4096         0.0.0.0:443        0.0.0.0:*
tcp   LISTEN 0      70           0.0.0.0:33060      0.0.0.0:*
tcp   LISTEN 0      4096         0.0.0.0:3000       0.0.0.0:*
tcp   LISTEN 0      151          0.0.0.0:3306       0.0.0.0:*
tcp   LISTEN 0      4096   127.0.0.53%lo:53         0.0.0.0:*
Chain INPUT (policy ACCEPT 14M packets, 2011M bytes)
 pkts bytes target     prot opt in     out     source               destination
```

## 4.4.3.3 Ensure ip6tables outbound and established connections are configured

### Info

Configure the firewall rules for new outbound, and established IPv6 connections.
Note:
- Changing firewall settings while connected over network can result in being locked out of the system
- Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well
If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

### Solution

Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:
# ip6tables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT # ip6tables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT # ip6tables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT # ip6tables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.13.1 |
| **800-171** | 3.13.5 |
| **800-171** | 3.13.6 |
| **800-171R3** | 03.13.01 |
| **800-171R3** | 03.13.06 |
| **800-53** | CA-9 |
| **800-53** | SC-7 |
| **800-53** | SC-7(5) |
| **800-53R5** | CA-9 |
| **800-53R5** | SC-7 |
| **800-53R5** | SC-7(5) |
| **CN-L3** | 7.1.2.2(c) |
| **CN-L3** | 8.1.10.6(j) |
| **CSCV7** | 9.4 |
| **CSCV8** | 4.4 |
| **CSCV8** | 4.5 |
| **CSF** | DE.CM-1 |
| **CSF** | ID.AM-3 |
| **CSF** | PR.AC-5 |
| **CSF** | PR.DS-5 |

| | |
|---|---|
| **CSF** | PR.PT-4 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | ID.AM-03 |
| **CSF2.0** | PR.DS-01 |
| **CSF2.0** | PR.DS-02 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **GDPR** | 32.1.d |
| **GDPR** | 32.2 |
| **HIPAA** | 164.306(a)(1) |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.8.16 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.13.1.3 |
| **ITSG-33** | SC-7 |
| **ITSG-33** | SC-7(5) |
| **LEVEL** | 1M |
| **NESA** | T4.5.4 |
| **NIAV2** | GS1 |
| **NIAV2** | GS2a |
| **NIAV2** | GS2b |
| **NIAV2** | GS7b |
| **NIAV2** | NS25 |
| **PCI-DSSV3.2.1** | 1.1 |
| **PCI-DSSV3.2.1** | 1.2 |
| **PCI-DSSV3.2.1** | 1.2.1 |
| **PCI-DSSV3.2.1** | 1.3 |
| **PCI-DSSV4.0** | 1.2.1 |
| **PCI-DSSV4.0** | 1.4.1 |
| **QCSC-V1** | 4.2 |

|  |  |
|---|---|
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 5.2.3 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 8.2.1 |
| **SWIFT-CSCV1** | 2.1 |
| **TBA-FIISB** | 43.1 |

## Assets

### linux_project

```
The command '/sbin/ip6tables -L -v -n' returned :

Chain INPUT (policy ACCEPT 12M packets, 1575M bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DOCKER-USER  0    --  *      *       ::/0                 ::/0
    0     0 DOCKER-FORWARD  0    --  *      *       ::/0                 ::/0

Chain OUTPUT (policy ACCEPT 198K packets, 1945M bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain DOCKER (0 references)
 pkts bytes target     prot opt in     out     source               destination

Chain DOCKER-BRIDGE (1 references)
 pkts bytes target     prot opt in     out     source               destination

Chain DOCKER-CT (1 references)
 pkts bytes target     prot opt in     out     source               destination

Chain DOCKER-FORWARD (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DOCKER-CT  0    --  *      *       ::/0                 ::/0
    0     0 DOCKER-ISOLATION-STAGE-1  0    --  *      *       ::/0                 ::/0

    0     0 DOCKER-BRIDGE  0    --  *      *       ::/0                 ::/0

Chain DOCKER-ISOLATION-STAGE-1 (1 references)
 pkts bytes target     prot opt in     out     source               destination

Chain DOCKER-ISOLATION-STAGE-2 (0 references)
 pkts bytes target     prot opt in     out     source               destination

Chain DOCKER-USER (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 RETURN     0    --  *      *       ::/0                 ::/0
```

## 5.1.6 Ensure sshd Ciphers are configured

### Info

This variable limits the ciphers that SSH can use during communication.
Notes:
- Some organizations may have stricter requirements for approved ciphers.
- Ensure that ciphers used are in compliance with site policy.
- The only "strong" ciphers currently FIPS 140 compliant are:
-
aes256-gcm@openssh.com
-
aes128-gcm@openssh.com
- aes256-ctr
- aes192-ctr
- aes128-ctr
Weak ciphers that are used for authentication to the cryptographic module cannot be relied upon to provide confidentiality or integrity, and system data may be compromised.
- The Triple DES ciphers, as used in SSH, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain clear text data via a birthday attack against a long-duration encrypted session, aka a "Sweet32" attack.
- Error handling in the SSH protocol; Client and Server, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plain text data from an arbitrary block of cipher text in an SSH session via unknown vectors.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

### Solution

Edit the /etc/ssh/sshd_config file and add/modify the Ciphers line to contain a comma separated list of the site unapproved (weak) Ciphers preceded with a - above any Include entries:
Example:
Ciphers -3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,chacha20-poly1305@openssh.com
- IF - CVE-2023-48795 has been addressed, and it meets local site policy, chacha20-poly1305@openssh.com may be removed from the list of excluded ciphers.
Note: First occurrence of an option takes precedence. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.13 |
| **800-171** | 3.5.2 |
| **800-171** | 3.13.8 |
| **800-171R3** | 03.05.07 |
| **800-171R3** | 03.05.12 |
| **800-171R3** | 03.13.08 |
| **800-53** | AC-17(2) |
| **800-53** | IA-5 |
| **800-53** | IA-5(1) |
| **800-53** | SC-8 |
| **800-53** | SC-8(1) |
| **800-53R5** | AC-17(2) |

| | |
|---|---|
| **800-53R5** | IA-5 |
| **800-53R5** | IA-5(1) |
| **800-53R5** | SC-8 |
| **800-53R5** | SC-8(1) |
| **CN-L3** | 7.1.2.7(g) |
| **CN-L3** | 7.1.3.1(d) |
| **CN-L3** | 8.1.2.2(a) |
| **CN-L3** | 8.1.2.2(b) |
| **CN-L3** | 8.1.4.1(c) |
| **CN-L3** | 8.1.4.7(a) |
| **CN-L3** | 8.1.4.8(a) |
| **CN-L3** | 8.2.4.5(c) |
| **CN-L3** | 8.2.4.5(d) |
| **CN-L3** | 8.5.2.2 |
| **CSCV7** | 14.4 |
| **CSCV8** | 3.10 |
| **CSF** | PR.AC-1 |
| **CSF** | PR.AC-3 |
| **CSF** | PR.DS-2 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-4 |
| **CSF2.0** | PR.AA-01 |
| **CSF2.0** | PR.AA-03 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-02 |
| **GDPR** | 32.1.a |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **HIPAA** | 164.312(a)(2)(i) |
| **HIPAA** | 164.312(d) |

| | |
|---|---|
| **HIPAA** | 164.312(e)(1) |
| **HIPAA** | 164.312(e)(2)(i) |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.14 |
| **ISO-27001-2022** | A.5.16 |
| **ISO-27001-2022** | A.5.17 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.6.7 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.2.2 |
| **ISO/IEC-27001** | A.10.1.1 |
| **ISO/IEC-27001** | A.13.2.3 |
| **ITSG-33** | AC-17(2) |
| **ITSG-33** | IA-5 |
| **ITSG-33** | IA-5(1) |
| **ITSG-33** | SC-8 |
| **ITSG-33** | SC-8a. |
| **ITSG-33** | SC-8(1) |
| **LEVEL** | 1A |
| **NESA** | T4.3.1 |
| **NESA** | T4.3.2 |
| **NESA** | T4.5.1 |
| **NESA** | T4.5.2 |
| **NESA** | T5.2.3 |
| **NESA** | T5.4.2 |
| **NESA** | T7.3.3 |
| **NESA** | T7.4.1 |
| **NIAV2** | AM37 |
| **NIAV2** | IE8 |
| **NIAV2** | IE9 |
| **NIAV2** | IE12 |

| | |
|---|---|
| **NIAV2** | NS5d |
| **NIAV2** | NS6b |
| **NIAV2** | NS29 |
| **NIAV2** | SS24 |
| **PCI-DSSV3.2.1** | 2.3 |
| **PCI-DSSV3.2.1** | 4.1 |
| **PCI-DSSV4.0** | 2.2.7 |
| **PCI-DSSV4.0** | 4.2.1 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.1 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 2.1 |
| **SWIFT-CSCV1** | 2.6 |
| **SWIFT-CSCV1** | 4.1 |
| **TBA-FIISB** | 29.1 |

## Assets

### linux_project

```
The command script with multiple lines returned :

port 22: ciphers chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
Pass
```

## 6.1.3.5 Ensure rsyslog logging is configured

### Info

The rsyslog and configuration files specifies rules for logging and which files are to be used to log certain classes of messages.
A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

### Solution

Edit the following lines in the configuration file(s) returned by the audit as appropriate for your environment.
Note: The below configuration is shown for example purposes only. Due care should be given to how the organization wishes to store log data.
*.emerg :omusrmsg:* auth,authpriv.* /var/log/secure mail.* -/var/log/mail mail.info -/var/log/mail.info mail.warning -/var/log/mail.warn mail.err /var/log/mail.err cron.* /var/log/cron
*.=warning;*.=err -/var/log/warn
*.crit /var/log/warn
*.*;mail.none;news.none -/var/log/messages local0,local1.* -/var/log/localmessages local2,local3.* -/var/log/localmessages local4,local5.* -/var/log/localmessages local6,local7.* -/var/log/localmessages
Run the following command to reload the rsyslogd configuration:
# systemctl reload-or-restart rsyslog

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.3.1 |
| **800-171** | 3.3.2 |
| **800-171** | 3.3.6 |
| **800-171R3** | 03.03.01 |
| **800-171R3** | 03.03.03 |
| **800-171R3** | 03.03.06a. |
| **800-53** | AU-2 |
| **800-53** | AU-7 |
| **800-53** | AU-12 |
| **800-53R5** | AU-2 |
| **800-53R5** | AU-7 |
| **800-53R5** | AU-12 |
| **CN-L3** | 7.1.2.3(c) |
| **CN-L3** | 8.1.4.3(a) |
| **CSCV7** | 6.2 |
| **CSCV7** | 6.3 |
| **CSCV8** | 8.2 |
| **CSF** | DE.CM-1 |
| **CSF** | DE.CM-3 |

| | |
|---|---|
| **CSF** | DE.CM-7 |
| **CSF** | PR.PT-1 |
| **CSF** | RS.AN-3 |
| **CSF2.0** | DE.CM-01 |
| **CSF2.0** | DE.CM-03 |
| **CSF2.0** | DE.CM-09 |
| **CSF2.0** | PR.PS-04 |
| **CSF2.0** | RS.AN-03 |
| **CSF2.0** | RS.AN-06 |
| **CSF2.0** | RS.AN-07 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.8.15 |
| **ITSG-33** | AU-2 |
| **ITSG-33** | AU-7 |
| **ITSG-33** | AU-12 |
| **LEVEL** | 1M |
| **NESA** | M1.2.2 |
| **NESA** | M5.5.1 |
| **NIAV2** | AM7 |
| **NIAV2** | AM11a |
| **NIAV2** | AM11b |
| **NIAV2** | AM11c |
| **NIAV2** | AM11d |
| **NIAV2** | AM11e |
| **NIAV2** | SS30 |
| **NIAV2** | VL8 |
| **PCI-DSSV3.2.1** | 10.1 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 6.2 |

| | |
|---|---|
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 10.2.1 |
| **QCSC-V1** | 11.2 |
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 6.4 |

## Assets

### linux_project

```
The command script with multiple lines returned :

/etc/rsyslog.d/50-default.conf:auth,authpriv.*   /var/log/auth.log
/etc/rsyslog.d/50-default.conf:*.*;auth,authpriv.none  -/var/log/syslog
/etc/rsyslog.d/50-default.conf:kern.*    -/var/log/kern.log
/etc/rsyslog.d/50-default.conf:mail.*    -/var/log/mail.log
/etc/rsyslog.d/50-default.conf:mail.err   /var/log/mail.err
```

## 6.1.3.8 Ensure logrotate is configured

### Info

The system includes the capability of rotating log files regularly to avoid filling up the system with logs or making the logs unmanageably large. The file /etc/logrotate.d/rsyslog is the configuration file used to rotate log files created by rsyslog
By keeping the log files smaller and more manageable, a system administrator can easily archive these files to another system and spend less time looking through inordinately large log files.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

### Solution

Edit /etc/logrotate.conf or the appropriate configuration file provided by the script in the Audit Procedure, as necessary to ensure logs are rotated according to site policy.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-53** | AU-4 |
| **800-53R5** | AU-4 |
| **CSCV7** | 6.4 |
| **CSCV8** | 8.3 |
| **CSF** | PR.DS-4 |
| **CSF** | PR.PT-1 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(b) |
| **ISO-27001-2022** | A.8.6 |
| **ITSG-33** | AU-4 |
| **LEVEL** | 1M |
| **NESA** | T3.3.1 |
| **NESA** | T3.6.2 |
| **QCSC-V1** | 8.2.1 |
| **QCSC-V1** | 13.2 |

### Assets

#### linux_project

```
 The command script with multiple lines returned :

# /etc/logrotate.conf
# see "man logrotate" for details

# global options do not affect preceding include directives

# rotate log files weekly
weekly

# use the adm group by default, since this is the owning group
# of /var/log/.
su root adm
```

```
# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
#dateext

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# system-specific logs may also be configured here.


# /etc/logrotate.d/alternatives
/var/log/alternatives.log {
 monthly
 rotate 12
 compress
 delaycompress
 missingok
 notifempty
 create 644 root root
}


# /etc/logrotate.d/apport
/var/log/apport.log {
       daily
       rotate 7
       delaycompress
       compress
       notifempty
       missingok
}



# /etc/logrotate.d/apt
/var/log/apt/term.log {
  rotate 12
  monthly
  compress
  missingok
  notifempty
}

/var/log/apt/history.log {
  rotate 12
  monthly
  compress
  missingok
  notifempty
}



# /etc/logrotate.d/bootlog
/var/log/boot.log
{
    missingok
    daily
    copytruncate
    rotate 7
    notifempty
}


# /etc/logrotate.d/btmp
# no packages own btmp -- we'll rotate it here
```

```
/var/log/btmp {
    missingok
    monthly
    create 0660 root utmp
    rotate 1
}


# /etc/logrotate.d/cloud-init
/var/log/cloud-init*.log
{
    su root root
    missingok
    nocreate
    notifempty
    rotate 6
    compress
    delaycompress
    size 1M
}


# /etc/logrotate.d/dpkg
/var/log/dpkg.log {
 monthly
 rotate 12
 compress
 delaycompress
 missingok
 notifempty
 create 644 root root
}


# /etc/logrotate.d/monarx-agent
/var/log/monarx-agent.log {
  rotate 12
  daily
  compress
  missingok
  notifempty
  create 600 root root
  size 100M
}


# /etc/logrotate.d/mysql-server
# - I put everything in one block and added sharedscripts, so that mysql gets
#   [...]
```

## 7.1.13 Ensure SUID and SGID files are reviewed

### Info

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SUID or SGID program is to enable users to perform functions (such as changing their password) that require root privileges.
There are valid reasons for SUID and SGID programs, but it is important to identify and review such programs to ensure they are legitimate. Review the files returned by the action in the audit section and check to see if system binaries have a different checksum than what from the package. This is an indication that the binary may have been replaced.
NOTE: Nessus has provided the target output to assist in reviewing the benchmark to ensure target compliance.

### Solution

Ensure that no rogue SUID or SGID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the integrity of these binaries.

### See Also

https://workbench.cisecurity.org/benchmarks/18959

### References

| | |
|---|---|
| **800-171** | 3.1.1 |
| **800-171** | 3.1.4 |
| **800-171** | 3.1.5 |
| **800-171** | 3.8.1 |
| **800-171** | 3.8.2 |
| **800-171** | 3.8.3 |
| **800-171R3** | 03.01.02 |
| **800-171R3** | 03.01.04 |
| **800-171R3** | 03.01.05a. |
| **800-171R3** | 03.08.02 |
| **800-53** | AC-3 |
| **800-53** | AC-5 |
| **800-53** | AC-6 |
| **800-53** | MP-2 |
| **800-53R5** | AC-3 |
| **800-53R5** | AC-5 |
| **800-53R5** | AC-6 |
| **800-53R5** | MP-2 |
| **CN-L3** | 7.1.3.2(b) |
| **CN-L3** | 7.1.3.2(g) |
| **CN-L3** | 8.1.4.2(d) |

| | |
|---|---|
| **CN-L3** | 8.1.4.2(f) |
| **CN-L3** | 8.1.4.11(b) |
| **CN-L3** | 8.1.10.2(c) |
| **CN-L3** | 8.1.10.6(a) |
| **CN-L3** | 8.5.3.1 |
| **CN-L3** | 8.5.4.1(a) |
| **CSCV7** | 14.6 |
| **CSCV8** | 3.3 |
| **CSF** | PR.AC-4 |
| **CSF** | PR.DS-5 |
| **CSF** | PR.PT-2 |
| **CSF** | PR.PT-3 |
| **CSF2.0** | PR.AA-05 |
| **CSF2.0** | PR.DS-10 |
| **CSF2.0** | PR.IR-01 |
| **GDPR** | 32.1.b |
| **HIPAA** | 164.306(a)(1) |
| **HIPAA** | 164.312(a)(1) |
| **ISO-27001-2022** | A.5.3 |
| **ISO-27001-2022** | A.5.10 |
| **ISO-27001-2022** | A.5.15 |
| **ISO-27001-2022** | A.5.33 |
| **ISO-27001-2022** | A.7.7 |
| **ISO-27001-2022** | A.7.10 |
| **ISO-27001-2022** | A.8.2 |
| **ISO-27001-2022** | A.8.3 |
| **ISO-27001-2022** | A.8.18 |
| **ISO-27001-2022** | A.8.20 |
| **ISO/IEC-27001** | A.6.1.2 |
| **ISO/IEC-27001** | A.9.4.1 |
| **ISO/IEC-27001** | A.9.4.5 |

| | |
|---|---|
| **ITSG-33** | AC-3 |
| **ITSG-33** | AC-5 |
| **ITSG-33** | AC-6 |
| **ITSG-33** | MP-2 |
| **ITSG-33** | MP-2a. |
| **LEVEL** | 1M |
| **NESA** | T1.3.2 |
| **NESA** | T1.3.3 |
| **NESA** | T1.4.1 |
| **NESA** | T4.2.1 |
| **NESA** | T5.1.1 |
| **NESA** | T5.2.2 |
| **NESA** | T5.4.1 |
| **NESA** | T5.4.4 |
| **NESA** | T5.4.5 |
| **NESA** | T5.5.4 |
| **NESA** | T5.6.1 |
| **NESA** | T7.5.2 |
| **NESA** | T7.5.3 |
| **NIAV2** | AM1 |
| **NIAV2** | AM3 |
| **NIAV2** | AM23f |
| **NIAV2** | SS13c |
| **NIAV2** | SS15c |
| **NIAV2** | SS29 |
| **PCI-DSSV3.2.1** | 7.1.2 |
| **PCI-DSSV4.0** | 7.2.1 |
| **PCI-DSSV4.0** | 7.2.2 |
| **QCSC-V1** | 3.2 |
| **QCSC-V1** | 5.2.2 |
| **QCSC-V1** | 6.2 |

| | |
|---|---|
| **QCSC-V1** | 13.2 |
| **SWIFT-CSCV1** | 5.1 |
| **TBA-FIISB** | 31.1 |
| **TBA-FIISB** | 31.4.2 |
| **TBA-FIISB** | 31.4.3 |

## Assets

### linux_project

```
The following 21 files are SUID or SGID:

  /usr/sbin/pam_extrausers_chkpwd
     owner: root, group: shadow, permissions: 2755

  /usr/sbin/unix_chkpwd
     owner: root, group: shadow, permissions: 2755

  /usr/lib/dbus-1.0/dbus-daemon-launch-helper
     owner: root, group: messagebus, permissions: 4754

  /usr/lib/x86_64-linux-gnu/utempter/utempter
     owner: root, group: utmp, permissions: 2755

  /usr/lib/polkit-1/polkit-agent-helper-1
     owner: root, group: root, permissions: 4755

  /usr/lib/snapd/snap-confine
     owner: root, group: root, permissions: 4755

  /usr/lib/openssh/ssh-keysign
     owner: root, group: root, permissions: 4755

  /usr/bin/sudo
     owner: root, group: root, permissions: 4755

  /usr/bin/ssh-agent
     owner: root, group: _ssh, permissions: 2755

  /usr/bin/gpasswd
     owner: root, group: root, permissions: 4755

  /usr/bin/chage
     owner: root, group: shadow, permissions: 2755

  /usr/bin/chfn
     owner: root, group: root, permissions: 4755

  /usr/bin/su
     owner: root, group: root, permissions: 4755

  /usr/bin/fusermount3
     owner: root, group: root, permissions: 4755

  /usr/bin/passwd
     owner: root, group: root, permissions: 4755

  /usr/bin/newgrp
     owner: root, group: root, permissions: 4755

  /usr/bin/expiry
     owner: root, group: shadow, permissions: 2755

  /usr/bin/mount
     owner: root, group: root, permissions: 4755

  /usr/bin/umount
     owner: root, group: root, permissions: 4755

  /usr/bin/chsh
```

```
   owner: root, group: root, permissions: 4755

/usr/bin/crontab
   owner: root, group: crontab, permissions: 2755
```