webfe_OS_upgradation

Ericsson DBSS0.6 BLK

Report generated by Nessus™ Sun, 30 Jun 2024 14:52:41 +06

TABLE OF CONTENTS

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Compliance 'FAILED'

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.

Rationale:

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 disable the cramfs module:

-IF- the module is available in the running kernel:

Create a file ending in .conf with install cramfs /bin/false in the /etc/modprobe.d/ directory

Create a file ending in .conf with blacklist cramfs in the /etc/modprobe.d/ directory

Unload cramfs from the kernel

-IF- available in ANY installed kernel:

Create a file ending in .conf with blacklist cramfs in the /etc/modprobe.d/ directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

No remediation is necessary

#!/usr/bin/env bash

{ l_mname='cramfs' # set module name l_mtype='fs' # set module type l_mpath='/lib/modules/**/kernel/$l_mtype'

l_mpname='$(tr '-' '_' <<< '$l_mname')'

l_mndir='$(tr '-' '/' <<< '$l_mname')'

module_loadable_fix() { # If the module is currently loadable, add 'install {MODULE_NAME} /bin/false' to a file in '/etc/modprobe.d'

l_loadable='$(modprobe -n -v '$l_mname')'

['$(wc -l <<< '$l_loadable')' -gt '1'] && l_loadable='$(grep -P -- '(^h*install|b$l_mname)b' <<< '$l_loadable')'

if ! grep -Pq -- '^h*install /bin/(true|false)' <<< '$l_loadable'; then echo -e '

- setting module: '$l_mname' to be not loadable'

echo -e 'install $l_mname /bin/false' >> /etc/modprobe.d/'$l_mpname'.conf fi } module_loaded_fix() { # If the module is currently loaded, unload the module if lsmod | grep '$l_mname' > /dev/null 2>&1; then echo -e '

- unloading module '$l_mname''

modprobe -r '$l_mname'

fi } module_deny_fix() { # If the module isn't deny listed, denylist the module if ! modprobe --showconfig | grep -Pq -- '^h*blacklisth+$l_mpnameb'; then echo -e '

- deny listing '$l_mname''

echo -e 'blacklist $l_mname' >> /etc/modprobe.d/'$l_mpname'.conf fi } # Check if the module exists on the system for l_mdir in $l_mpath; do if [-d '$l_mdir/$l_mndir'] && [-n '$(ls -A $l_mdir/$l_mndir)']; then echo -e '

- module: '$l_mname' exists in '$l_mdir'

- checking if disabled...'

module_deny_fix if ['$l_mdir' = '/lib/modules/$(uname -r)/kernel/$l_mtype']; then module_loadable_fix module_loaded_fix fi else echo -e '

- module: '$l_mname' doesn't exist in '$l_mdir'

'

fi done echo -e '

- remediation of module: '$l_mname' complete '

}

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

-- INFO --
 - module: "cramfs" exists in:
  - "/lib/modules/4.18.0-513.24.1.el8_9.x86_64/kernel/fs"
  - "/lib/modules/5.4.17-2136.330.7.1.el8uek.x86_64/kernel/fs"

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:

 - module: "cramfs" is not deny listed
 - module: "cramfs" is loadable: "insmod /lib/modules/4.18.0-513.24.1.el8_9.x86_64/kernel/fs/cramfs/
cramfs.ko.xz "


- Correctly set:

 - module: "cramfs" is not loaded
```

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.

Rationale:

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 disable the jffs2 module:

-IF- the module is available in the running kernel:

Create a file ending in .conf with install jffs2 /bin/false in the /etc/modprobe.d/ directory

Create a file ending in .conf with blacklist jffs2 in the /etc/modprobe.d/ directory

Unload jffs2 from the kernel

-IF- available in ANY installed kernel:

Create a file ending in .conf with blacklist jffs2 in the /etc/modprobe.d/ directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

No remediation is necessary

#!/usr/bin/env bash

{ l_mname='jffs2' # set module name l_mtype='fs' # set module type l_mpath='/lib/modules/**/kernel/$l_mtype'

l_mpname='$(tr '-' '_' <<< '$l_mname')'

l_mndir='$(tr '-' '/' <<< '$l_mname')'

module_loadable_fix() { # If the module is currently loadable, add 'install {MODULE_NAME} /bin/false' to a file in '/etc/modprobe.d'

l_loadable='$(modprobe -n -v '$l_mname')'

['$(wc -l <<< '$l_loadable')' -gt '1'] && l_loadable='$(grep -P -- '(^h*install|b$l_mname)b' <<< '$l_loadable')'

if ! grep -Pq -- '^h*install /bin/(true|false)' <<< '$l_loadable'; then echo -e '

- setting module: '$l_mname' to be not loadable'

echo -e 'install $l_mname /bin/false' >> /etc/modprobe.d/'$l_mpname'.conf fi } module_loaded_fix() { # If the module is currently loaded, unload the module if lsmod | grep '$l_mname' > /dev/null 2>&1; then echo -e '

- unloading module '$l_mname''

modprobe -r '$l_mname'

fi } module_deny_fix() { # If the module isn't deny listed, denylist the module if ! modprobe --showconfig | grep -Pq -- '^h*blacklisth+$l_mpnameb'; then echo -e '

- deny listing '$l_mname''

echo -e 'blacklist $l_mname' >> /etc/modprobe.d/'$l_mpname'.conf fi } # Check if the module exists on the system for l_mdir in $l_mpath; do if [-d '$l_mdir/$l_mndir'] && [-n '$(ls -A $l_mdir/$l_mndir)']; then echo -e '

- module: '$l_mname' exists in '$l_mdir'

- checking if disabled...'

module_deny_fix if ['$l_mdir' = '/lib/modules/$(uname -r)/kernel/$l_mtype']; then module_loadable_fix module_loaded_fix fi else echo -e '

- module: '$l_mname' doesn't exist in '$l_mdir'

'

fi done echo -e '

- remediation of module: '$l_mname' complete '

}

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

-- INFO --
 - module: "jffs2" exists in:
  - "/lib/modules/5.4.17-2136.330.7.1.el8uek.x86_64/kernel/fs"

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:

 - module: "jffs2" is not deny listed


- Correctly set:

 - module: "jffs2" doesn't exist in "/lib/modules/4.18.0-513.24.1.el8_9.x86_64/kernel/fs"
```

1.1.1.8 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.

Rationale:

Restricting USB access on the system will decrease the physical attack surface for a device and diminish the possible vectors to introduce malware.

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.

Solution

Run the following script to disable the usb-storage module:

-IF- the module is available in the running kernel:

Create a file ending in .conf with install usb-storage /bin/false in the /etc/modprobe.d/ directory

Create a file ending in .conf with blacklist usb-storage in the /etc/modprobe.d/ directory

Unload usb-storage from the kernel

-IF- available in ANY installed kernel:

Create a file ending in .conf with blacklist usb-storage in the /etc/modprobe.d/ directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

No remediation is necessary

#!/usr/bin/env bash

{ l_mname='usb-storage' # set module name l_mtype='drivers' # set module type l_mpath='/lib/modules/**/kernel/$l_mtype'

l_mpname='$(tr '-' '_' <<< '$l_mname')'

l_mndir='$(tr '-' '/' <<< '$l_mname')'

module_loadable_fix() { # If the module is currently loadable, add 'install {MODULE_NAME} /bin/false' to a file in '/etc/modprobe.d'

l_loadable='$(modprobe -n -v '$l_mname')'

['$(wc -l <<< '$l_loadable')' -gt '1'] && l_loadable='$(grep -P -- '(^h*install|b$l_mname)b' <<< '$l_loadable')'

if ! grep -Pq -- '^h*install /bin/(true|false)' <<< '$l_loadable'; then echo -e '

- setting module: '$l_mname' to be not loadable'

echo -e 'install $l_mname /bin/false' >> /etc/modprobe.d/'$l_mpname'.conf fi } module_loaded_fix() { # If the module is currently loaded, unload the module if lsmod | grep '$l_mname' > /dev/null 2>&1; then echo -e '

- unloading module '$l_mname''

modprobe -r '$l_mname'

fi } module_deny_fix() { # If the module isn't deny listed, denylist the module if ! modprobe --showconfig | grep -Pq -- '^h*blacklisth+$l_mpnameb'; then echo -e '

- deny listing '$l_mname''

echo -e 'blacklist $l_mname' >> /etc/modprobe.d/'$l_mpname'.conf fi } # Check if the module exists on the system for l_mdir in $l_mpath; do if [-d '$l_mdir/$l_mndir'] && [-n '$(ls -A $l_mdir/$l_mndir)']; then echo -e '

- module: '$l_mname' exists in '$l_mdir'

- checking if disabled...'

module_deny_fix if ['$l_mdir' = '/lib/modules/$(uname -r)/kernel/$l_mtype']; then module_loadable_fix module_loaded_fix fi else echo -e '

- module: '$l_mname' doesn't exist in '$l_mdir'

'

fi done echo -e '

- remediation of module: '$l_mname' complete '

}

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.8.7
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/IEC-27001	A.8.3.1
ISO/IEC-27001	A.8.3.3
LEVEL	1A
LEVEL	2A
NESA	T1.4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

-- INFO --
 - module: "usb-storage" exists in:
  - "/lib/modules/4.18.0-513.24.1.el8_9.x86_64/kernel/drivers"
  - "/lib/modules/5.4.17-2136.330.7.1.el8uek.x86_64/kernel/drivers"

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:

 - module: "usb-storage" is not deny listed
 - module: "usb-storage" is loadable: "insmod /lib/modules/4.18.0-513.24.1.el8_9.x86_64/kernel/
drivers/usb/storage/usb-storage.ko.xz "


- Correctly set:

 - module: "usb-storage" is not loaded
```

1.2.2 Ensure gpgcheck is globally activated

Info

The gpgcheck option, found in the main section of the /etc/dnf/dnf.conf and individual /etc/yum.repos.d/* files, determines if an RPM package's signature is checked prior to its installation.

Rationale:

It is important to ensure that an RPM's package signature is always checked prior to installation to ensure that the software is obtained from a trusted source.

Solution

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

Example:

sed -i 's/^gpgchecks*=s*.*/gpgcheck=1/' /etc/dnf/dnf.conf

Edit any failing files in /etc/yum.repos.d/* and set all instances starting with gpgcheck to 1.

Example:

find /etc/yum.repos.d/ -name '*.repo' -exec echo 'Checking:' {} ; -exec sed -i 's/^gpgchecks*=s*.*/ gpgcheck=1/' {} ;

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.11.2
800-171	3.11.3
800-171	3.14.1
800-53	RA-5
800-53	SI-2
800-53	SI-2(2)
800-53R5	RA-5
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

CSCV8	7.3
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
GDPR	32.1.b
GDPR	32.1.d
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.6.1
ITSG-33	RA-5
ITSG-33	SI-2
ITSG-33	SI-2(2)
LEVEL	1A
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
PASSED - Global configuration is set correctly
Compliant file(s):
      /etc/dnf/dnf.conf - regex '^[\s]*gpgcheck[\s]*=' found - expect
 '^[\s]*gpgcheck[\s]*=[\s]*1[\s]*$' found in the following lines:
          2: gpgcheck=1

-------------------------
FAILED - yum.repos.d configuration is set correctly
File permission denied: /etc/yum.repos.d/local-oracle-linux-ol8.repo
```

1.2.5 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.

Rationale:

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

Solution

Use your package manager to update all packages on the system according to site policy.

The following command will install all available updates:

dnf update

Once the update process is complete, verify if reboot is required to load changes.

dnf needs-restarting -r

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.11.2
800-171	3.11.3
800-171	3.14.1
800-53	RA-5
800-53	SI-2
800-53	SI-2(2)
800-53R5	RA-5
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

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
GDPR	32.1.b
GDPR	32.1.d
HIPAA	164.306(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
PASSED - Check to make sure no system reboot is required
The command '/bin/dnf needs-restarting -r' returned :

No core libraries or services have been updated since boot-up.
Reboot should not be necessary.

-------------------------
FAILED - Ensure updates, patches, and additional security software are installed
The command '/bin/dnf check-update | /bin/awk '{print} END {if (NR == 1) print "pass"; else print}''
 returned :

Error: There are no enabled repositories in "/etc/yum.repos.d", "/etc/yum/repos.d", "/etc/
distro.repos.d".
```

1.3.1 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.

Rationale:

Requiring a boot password upon execution of the boot loader will prevent an unauthorized user from entering boot parameters or changing the boot partition. This prevents users from weakening security (e.g. turning off SELinux at boot time).

Impact:

If password protection is enabled, only the designated superuser can edit a GRUB 2 menu item by pressing e or access the GRUB 2 command line by pressing c

If GRUB 2 is set up to boot automatically to a password-protected menu entry the user has no option to back out of the password prompt to select another menu entry. Holding the SHIFT key will not display the menu in this case. The user must enter the correct username and password. If unable, the configuration files will have to be edited via the LiveCD or other means to fix the problem

Solution

Create an encrypted password with grub2-setpassword:

grub2-setpassword

Enter password: <password>

Confirm password: <password>

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: GRUB2_PASSWORD=grub.pbkdf2.sha512 timeout: 7200

Hosts

10.74.6.135

```
The command script with multiple lines returned :

find: '/boot/efi': Permission denied
find: '/boot/grub2': Permission denied
find: '/boot/loader/entries': Permission denied
```

1.4.1 Ensure address space layout randomization (ASLR) 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.

Rationale:

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 in .conf:

kernel.randomize_va_space = 2

Example:

printf '

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

Default Value:

kernel.randomize_va_space = 2

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-53	SI-16
800-53R5	SI-16
CSCV7	8.3
CSCV8	10.5
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	SI-16
LEVEL	1A

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied

- 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
```

1.4.2 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.

Rationale:

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

kernel.yama.ptrace_scope = 1

Example:

printf '

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 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/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:

 - "kernel.yama.ptrace_scope" is not set in an included file
   ** Note: "kernel.yama.ptrace_scope" May be set in a file that's ignored by load procedure **



- Correctly set:

 - "kernel.yama.ptrace_scope" is correctly set to "1" in the running configuration
```

1.5.1.6 Ensure no unconfined services exist

Info

Unconfined processes run in unconfined domains

Rationale:

For unconfined processes, SELinux policy rules are applied, but policy rules exist that allow processes running in unconfined domains almost all access. Processes running in unconfined domains fall back to using DAC rules exclusively. If an unconfined process is compromised, SELinux does not prevent an attacker from gaining access to system resources and data, but of course, DAC rules are still used. SELinux is a security enhancement on top of DAC rules - it does not replace them

Solution

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

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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	9.2
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: /bin/ps -eZ | /bin/grep unconfined_service_t | /bin/awk -F: '{ print $NF } END {if (NR == 0) print "none"}'

expect: ^none$

Hosts

10.74.6.135

```
The command '/bin/ps -eZ | /bin/grep unconfined_service_t | /bin/awk -F: '{ print $NF } END {if (NR
 == 0) print "none"}'' returned :

46 java
19 nrpe
33 filebeat
44 netdata
25 go.d.plugin
02 python
37 apps.plugin
01 bash
00 consul-template
00 SetroubleshootP
```

1.7.1 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

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the ' uname -a ' command once they have logged in.

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/15289

References

800-171	3.1.9
800-53	AC-8a.
800-53R5	AC-8a.
GDPR	32.1.b
HIPAA	164.306(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
FAILED - mrsv not included in /etc/motd
File permission denied: /etc/motd

-------------------------
FAILED - banner text
File permission denied: /etc/motd
```

1.7.2 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

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the ' uname -a ' command once they have logged in.

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/15289

References

800-171	3.1.9
800-53	AC-8
800-53R5	AC-8
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	AC-8
LEVEL	1A
NESA	M1.3.6
TBA-FIISB	45.2.4

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

------------------------
FAILED - banner text
File permission denied: /etc/issue

------------------------
FAILED - mrsv not included in /etc/issue
File permission denied: /etc/issue
```

1.7.3 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

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the ' uname -a ' command once they have logged in.

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/15289

References

800-171	3.1.9
800-53	AC-8
800-53R5	AC-8
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	AC-8
LEVEL	1A
NESA	M1.3.6
TBA-FIISB	45.2.4

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

------------------------
PASSED - mrsv not included in /etc/issue.net
The file "/etc/issue.net" does not contain "\\[mrsv]"

------------------------
FAILED - banner text
First ERROR: ############################################################################## # != All
 activities
##############################################################################
# Unauthorized access is prohibited
##############################################################################
```

2.1.2 Ensure chrony is configured

Info

chrony is a daemon which implements the Network Time Protocol (NTP) and is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. More information on chrony can be found at http://chrony.tuxfamily.org/. chrony can be configured to be a client and/or a server.

Rationale:

If chrony is in use on the system proper configuration is vital to ensuring time synchronization is working properly.

Solution

Add or edit server or pool lines to /etc/chrony.conf or a file in the /etc/chrony.d directory as appropriate:

Example:

server <remote-server>

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.6
800-171	3.3.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: ^[\s]*(server|pool)[\s]+10\.0\.0\.2 file: /etc/chrony.conf /etc/chrony.d/* min_occurrences: 1 regex: ^[\s]*(server|pool)[\s]+10\.0\.0\.2 string_required: NO

Hosts

10.74.6.135

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

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.

Rationale:

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.

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.

Solution

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

net.ipv4.ip_forward = 0

Example:

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

Run the following command to set the active kernel parameters:

{ 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 in .conf:

net.ipv6.conf.all.forwarding = 0

Example:

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

Run the following command to set the active kernel parameters:

{ 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

Default Value:

net.ipv4.ip_forward = 0

net.ipv6.conf.all.forwarding = 0

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied
Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied

- Audit Result:
  ** FAIL **
```

```
  - Reason(s) for audit failure:

  - "net.ipv4.ip_forward" is not set in an included file
    ** Note: "net.ipv4.ip_forward" May be set in a file that's ignored by load procedure **

  - "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.ipv4.ip_forward" is correctly set to "0" in the running configuration
  - "net.ipv6.conf.all.forwarding" is correctly set to "0" in the running configuration
```

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.

Rationale:

An attacker could use a compromised host to send invalid ICMP redirects to other router devices in an attempt to corrupt routing and have users access a system set up by the attacker as opposed to a valid system.

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.

Solution

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

net.ipv4.conf.all.send_redirects = 0

net.ipv4.conf.default.send_redirects = 0

Example:

printf '

net.ipv4.conf.all.send_redirects = 0 net.ipv4.conf.default.send_redirects = 0 ' >> /etc/sysctl.d/60-netipv4_sysctl.conf

Run the following command to set the active kernel parameters:

{ sysctl -w net.ipv4.conf.all.send_redirects=0 sysctl -w net.ipv4.conf.default.send_redirects=0 sysctl -w net.ipv4.route.flush=1 }

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

Default Value:

net.ipv4.conf.all.send_redirects = 1

net.ipv4.conf.default.send_redirects = 1

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2

800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied
Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:

 - "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 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 **



- Correctly set:

 - "net.ipv4.conf.all.send_redirects" is correctly set to "0" in the running configuration
```

```
- "net.ipv4.conf.default.send_redirects" is correctly set to "0" in the running configuration
```

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.

Rationale:

Some routers (and some attackers) will send responses that violate RFC-1122 and attempt to fill up a log file system with many useless error messages.

Solution

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

net.ipv4.icmp_ignore_bogus_error_responses = 1

Example:

printf '

net.ipv4.icmp_ignore_bogus_error_responses = 1 ' >> /etc/sysctl.d/60-netipv4_sysctl.conf

Run the following command to set the active kernel parameters:

{ 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

Default Value:

net.ipv4.icmp_ignore_bogus_error_responses = 1

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:

 - "net.ipv4.icmp_ignore_bogus_error_responses" is not set in an included file
   ** Note: "net.ipv4.icmp_ignore_bogus_error_responses" May be set in a file that's ignored by load
 procedure **



- Correctly set:

 - "net.ipv4.icmp_ignore_bogus_error_responses" is correctly set to "1" in the running configuration
```

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.

Rationale:

Accepting ICMP echo and timestamp requests with broadcast or multicast destinations for your network could be used to trick your host into starting (or participating) in a Smurf attack. A Smurf attack relies on an attacker sending large amounts of ICMP broadcast messages with a spoofed source address. All hosts receiving this message and responding would send echo-reply messages back to the spoofed address, which is probably not routable. If many hosts respond to the packets, the amount of traffic on the network could be significantly multiplied.

Solution

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

net.ipv4.icmp_echo_ignore_broadcasts = 1

Example:

printf '

net.ipv4.icmp_echo_ignore_broadcasts = 1 ' >> /etc/sysctl.d/60-netipv4_sysctl.conf

Run the following command to set the active kernel parameters:

{ 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

Default Value:

net.ipv4.conf.default.log_martians = 0

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:

 - "net.ipv4.icmp_echo_ignore_broadcasts" is not set in an included file
   ** Note: "net.ipv4.icmp_echo_ignore_broadcasts" May be set in a file that's ignored by load
 procedure **



- Correctly set:

 - "net.ipv4.icmp_echo_ignore_broadcasts" is correctly set to "1" in the running configuration
```

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.

Rationale:

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 in .conf:

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

Example:

printf '

net.ipv4.conf.all.accept_redirects = 0 net.ipv4.conf.default.accept_redirects = 0 ' >> /etc/sysctl.d/60-netipv4_sysctl.conf

Run the following command to set the active kernel parameters:

{ sysctl -w net.ipv4.conf.all.accept_redirects=0 sysctl -w net.ipv4.conf.default.accept_redirects=0 sysctl -w net.ipv4.route.flush=1 }

-IF- IPv6 is enabled on the system:

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

net.ipv6.conf.all.accept_redirects = 0

net.ipv6.conf.default.accept_redirects = 0

Example:

printf '

net.ipv6.conf.all.accept_redirects = 0 net.ipv6.conf.default.accept_redirects = 0 ' >> /etc/sysctl.d/60-netipv6_sysctl.conf

Run the following command to set the active kernel parameters:

{ sysctl -w net.ipv6.conf.all.accept_redirects=0 sysctl -w net.ipv6.conf.default.accept_redirects=0 sysctl -w net.ipv6.route.flush=1 }

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

Default Value:

net.ipv4.conf.all.accept_redirects = 1

net.ipv4.conf.default.accept_redirects = 1

net.ipv6.conf.all.accept_redirects = 1

net.ipv6.conf.default.accept_redirects = 1

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied
Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied
Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied
Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:

 - "net.ipv4.conf.all.accept_redirects" is not set in an included file
   ** Note: "net.ipv4.conf.all.accept_redirects" May be set in a file that's ignored by load
 procedure **

 - "net.ipv4.conf.default.accept_redirects" is not set in an included file
   ** Note: "net.ipv4.conf.default.accept_redirects" May be set in a file that's ignored by load
 procedure **

 - "net.ipv6.conf.all.accept_redirects" is not set in an included file
   ** Note: "net.ipv6.conf.all.accept_redirects" May be set in a file that's ignored by load
 procedure **

 - "net.ipv6.conf.default.accept_redirects" is not set in an included file
   ** Note: "net.ipv6.conf.default.accept_redirects" May be set in a file that's ignored by load
 procedure **



- Correctly set:

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

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.

Rationale:

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 in .conf:

net.ipv4.conf.all.secure_redirects = 0

net.ipv4.conf.default.secure_redirects = 0

Example:

printf '

net.ipv4.conf.all.secure_redirects = 0 net.ipv4.conf.default.secure_redirects = 0 ' >> /etc/sysctl.d/60-netipv4_sysctl.conf

Run the following commands to set the active kernel parameters:

{ sysctl -w net.ipv4.conf.all.secure_redirects=0 sysctl -w net.ipv4.conf.default.secure_redirects=0 sysctl -w net.ipv4.route.flush=1 }

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

Default Value:

net.ipv4.conf.all.secure_redirects = 1

net.ipv4.conf.default.secure_redirects = 1

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied
Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:

 - "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 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 **



- Correctly set:

 - "net.ipv4.conf.all.secure_redirects" is correctly set to "0" in the running configuration
 - "net.ipv4.conf.default.secure_redirects" is correctly set to "0" in the running configuration
```

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).

Rationale:

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.

Impact:

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 in .conf:

net.ipv4.conf.all.rp_filter = 1

net.ipv4.conf.default.rp_filter = 1

Example:

# printf '
net.ipv4.conf.all.rp_filter = 1 net.ipv4.conf.default.rp_filter = 1 ' >> /etc/sysctl.d/60-netipv4_sysctl.conf

Run the following commands to set the active kernel parameters:

{ sysctl -w net.ipv4.conf.all.rp_filter=1 sysctl -w net.ipv4.conf.default.rp_filter=1 sysctl -w net.ipv4.route.flush=1 }

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

Default Value:

net.ipv4.conf.all.rp_filter = 2

net.ipv4.conf.default.rp_filter = 1

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied
Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:

 - "net.ipv4.conf.default.rp_filter" is not set in an included file
   ** Note: "net.ipv4.conf.default.rp_filter" May be set in a file that's ignored by load procedure
 **



- Correctly set:

 - "net.ipv4.conf.all.rp_filter" is correctly set to "1" in the running configuration
```

```
- "net.ipv4.conf.all.rp_filter" is correctly set to "1" in "/usr/lib/sysctl.d/50-default.conf"
- "net.ipv4.conf.default.rp_filter" is correctly set to "1" in the running configuration
```

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.

Rationale:

Setting net.ipv4.conf.all.accept_source_route, net.ipv4.conf.default.accept_source_route, net.ipv6.conf.all.accept_source_route and net.ipv6.conf.default.accept_source_route to 0 disables the system from accepting source routed packets. Assume this system was capable of routing packets to Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

Solution

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

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

Example:

printf '

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 command to set the active kernel parameters:

{ sysctl -w net.ipv4.conf.all.accept_source_route=0 sysctl -w net.ipv4.conf.default.accept_source_route=0 sysctl -w net.ipv4.route.flush=1 }

-IF- IPv6 is enabled on the system:

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

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0

Example:

printf '

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:

{ 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

Default Value:

net.ipv4.conf.all.accept_source_route = 0

net.ipv4.conf.default.accept_source_route = 0

net.ipv6.conf.all.accept_source_route = 0

net.ipv6.conf.default.accept_source_route = 0

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied
Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied
Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied
Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:

 - "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.ipv4.conf.all.accept_source_route" is correctly set to "0" in "/usr/lib/sysctl.d/50-
default.conf"

 - "net.ipv4.conf.default.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.

Rationale:

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 in .conf:

net.ipv4.conf.all.log_martians = 1

net.ipv4.conf.default.log_martians = 1

Example:

printf '

net.ipv4.conf.all.log_martians = 1 net.ipv4.conf.default.log_martians = 1 ' >> /etc/sysctl.d/60-netipv4_sysctl.conf

Run the following command to set the active kernel parameters:

{ sysctl -w net.ipv4.conf.all.log_martians=1 sysctl -w net.ipv4.conf.default.log_martians=1 sysctl -w net.ipv4.route.flush=1 }

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

Default Value:

net.ipv4.conf.all.log_martians = 0

net.ipv4.conf.default.log_martians = 0

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied
Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:

 - "net.ipv4.conf.all.log_martians" is not set in an included file
   ** Note: "net.ipv4.conf.all.log_martians" May be set in a file that's ignored by load procedure
 **

 - "net.ipv4.conf.default.log_martians" is not set in an included file
   ** Note: "net.ipv4.conf.default.log_martians" May be set in a file that's ignored by load
 procedure **



- Correctly set:

 - "net.ipv4.conf.all.log_martians" is correctly set to "1" in the running configuration
 - "net.ipv4.conf.default.log_martians" is correctly set to "1" 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.

Rationale:

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 in .conf:

net.ipv4.tcp_syncookies = 1

Example:

printf '

net.ipv4.tcp_syncookies = 1 ' >> /etc/sysctl.d/60-netipv4_sysctl.conf

Run the following command to set the active kernel parameters:

{ 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

Default Value:

net.ipv4.tcp_syncookies = 1

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7

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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied

- 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

This setting disables the system's ability to accept IPv6 router advertisements.

Rationale:

It is recommended that systems do not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes. 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 in .conf:

net.ipv6.conf.all.accept_ra = 0

net.ipv6.conf.default.accept_ra = 0

Example:

printf '

net.ipv6.conf.all.accept_ra = 0 net.ipv6.conf.default.accept_ra = 0 ' >> /etc/sysctl.d/60-netipv6_sysctl.conf

Run the following command to set the active kernel parameters:

{ sysctl -w net.ipv6.conf.all.accept_ra=0 sysctl -w net.ipv6.conf.default.accept_ra=0 sysctl -w net.ipv6.route.flush=1 }

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

Default Value:

net.ipv6.conf.all.accept_ra = 1

net.ipv6.conf.default.accept_ra = 1

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied
Failed to cat /etc/sysctl.d/60-kernel_sysctl.conf: Permission denied

- Audit Result:
  ** FAIL **
 - Reason(s) for audit failure:

 - "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 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
 **



- Correctly set:

 - "net.ipv6.conf.all.accept_ra" is correctly set to "0" in the running configuration
 - "net.ipv6.conf.default.accept_ra" is correctly set to "0" in the running configuration
```

3.4.2.1 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.

Rationale:

If a base chain doesn't exist with a hook for input, forward, and delete, packets that would flow through those chains will not be touched by nftables.

Impact:

If configuring 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

Solution

- IF not using FirewallD - 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 ; }

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
FAILED - hook output
The command '/sbin/nft -n list ruleset | /bin/grep 'hook output'' returned :

Operation not permitted (you must be root)

-------------------------
FAILED - hook input
The command '/sbin/nft -n list ruleset | /bin/grep 'hook input'' returned :

Operation not permitted (you must be root)

-------------------------
FAILED - hook forward
The command '/sbin/nft -n list ruleset | /bin/grep 'hook forward'' returned :

Operation not permitted (you must be root)
```

3.4.2.2 Ensure host based firewall loopback traffic is configured

Info

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Solution

Run the following script to implement the loopback rules:

#!/usr/bin/env bash

{ l_hbfw=''

if systemctl is-enabled firewalld.service | grep -q 'enabled' && systemctl is-enabled nftables.service | grep -q 'enabled'; then echo -e '

- Error - Both FirewallD and NFTables are enabled

- Please follow recommendation: 'Ensure a single firewall configuration utility is in use''

elif ! systemctl is-enabled firewalld.service | grep -q 'enabled' && ! systemctl is-enabled nftables.service | grep -q 'enabled'; then echo -e '

- Error - Neither FirewallD or NFTables is enabled

- Please follow recommendation: 'Ensure a single firewall configuration utility is in use''

else if systemctl is-enabled firewalld.service | grep -q 'enabled' && ! systemctl is-enabled nftables.service | grep -q 'enabled'; then echo -e '

- FirewallD is in use on the system' && l_hbfw='fwd'

elif ! systemctl is-enabled firewalld.service | grep -q 'enabled' && systemctl is-enabled nftables.service | grep -q 'enabled'; then echo -e '

- NFTables is in use on the system' && l_hbfw='nft'

fi l_ipsaddr='$(nft list ruleset | awk '/filter_IN_public_deny|hooks+inputs+/,/}s*(#.*)?$/' | grep -P -- 'iph +saddr')'

if ! nft list ruleset | awk '/hooks+inputs+/,/}s*(#.*)?$/' | grep -Pq -- 'H+h+'lo'h+accept'; then echo -e '

- Enabling input to accept for loopback address'

if ['$l_hbfw' = 'fwd']; then firewall-cmd --permanent --zone=trusted --add-interface=lo firewall-cmd --reload elif ['$l_hbfw' = 'nft']; then nft add rule inet filter input iif lo accept fi fi if ! grep -Pq -- 'iph+saddrh +127.0.0.0/8h+(counterh+packetsh+d+h+bytesh+d+h+)?drop' <<< '$l_ipsaddr' && ! grep -Pq -- 'iph+daddrh +!=h+127.0.0.1h+iph+saddrh+127.0.0.1h+drop' <<< '$l_ipsaddr'; then echo -e '

- Setting IPv4 network traffic from loopback address to drop'

if ['$l_hbfw' = 'fwd']; then firewall-cmd --permanent --add-rich-rule='rule family=ipv4 source address='127.0.0.1' destination not address='127.0.0.1' drop'

firewall-cmd --permanent --zone=trusted --add-rich-rule='rule family=ipv4 source address='127.0.0.1' destination not address='127.0.0.1' drop'

firewall-cmd --reload elif ['$l_hbfw' = 'nft']; then nft create rule inet filter input ip saddr 127.0.0.0/8 counter drop fi fi if grep -Pq -- '^h*0h*$' /sys/module/ipv6/parameters/disable; then l_ip6saddr='$(nft list ruleset | awk '/filter_IN_public_deny|hook input/,/}/' | grep 'ip6 saddr')'

if ! grep -Pq 'ip6h+saddrh+::1h+(counterh+packetsh+d+h+bytesh+d+h+)?drop' <<< '$l_ip6saddr' && ! grep -Pq -- 'ip6h+daddrh+!=h+::1h+ip6h+saddrh+::1h+drop' <<< '$l_ip6saddr'; then echo -e '

- Setting IPv6 network traffic from loopback address to drop'

if ['$l_hbfw' = 'fwd']; then firewall-cmd --permanent --add-rich-rule='rule family=ipv6 source address='::1' destination not address='::1' drop'

firewall-cmd --permanent --zone=trusted --add-rich-rule='rule family=ipv6 source address='::1' destination not address='::1' drop'

firewall-cmd --reload elif ['$l_hbfw' = 'nft']; then nft add rule inet filter input ip6 saddr ::1 counter drop fi fi fi fi }

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

Operation not permitted (you must be root)
Operation not permitted (you must be root)
Operation not permitted (you must be root)

- Audit Result:
  *** FAIL ***

 - Network traffic to the loopback address is not set to accept
 - IPv4 network traffic from loopback address not set to drop
 - IPv6 network traffic from loopback address not set to drop

  - Correctly set:
```

4.2.2 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.

Rationale:

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

{ l_output='' l_output2=''

l_skgn='$(grep -Po -- '^(ssh_keys|_?ssh)b' /etc/group)' # Group designated to own openSSH keys
l_skgid='$(awk -F: '($1 == "'$l_skgn'"){print $3}' /etc/group)' # Get gid of group if [-n '$l_skgid']; then
l_agroup='(root|$l_skgn)' && l_sgroup='$l_skgn' && l_mfix='u-x,g-wx,o-rwx'

else l_agroup='root' && l_sgroup='root' && l_mfix='u-x,go-rwx'

fi unset a_skarr && a_skarr=() # Clear and initialize array if [-d /etc/ssh]; then while IFS= read -r -d $'0' l_file; do # Loop to populate array if grep -Pq ':h+OpenSSHh+privateh+keyb' <<< '$(file '$l_file')'; then a_skarr +=('$(stat -Lc '%n^%#a^%U^%G^%g' '$l_file')') fi done < <(find -L /etc/ssh -xdev -type f -print0) while IFS='^' read -r l_file l_mode l_owner l_group l_gid; do l_out2=''

['$l_gid' = '$l_skgid'] && l_pmask='0137' || l_pmask='0177'

l_maxperm='$(printf '%o' $((0777 & ~$l_pmask)))'

if [$(($l_mode & $l_pmask)) -gt 0]; then l_out2='$l_out2

- Mode: '$l_mode' should be mode: '$l_maxperm' or more restrictive

- Revoking excess permissions'

chmod '$l_mfix' '$l_file'

fi if ['$l_owner' != 'root']; then l_out2='$l_out2

- Owned by: '$l_owner' should be owned by 'root'

- Changing ownership to 'root''

chown root '$l_file'

fi if [[! '$l_group' =~ $l_agroup]]; then l_out2='$l_out2

- Owned by group '$l_group' should be group owned by: '${l_agroup//|/ or }'

- Changing group ownership to '$l_sgroup''

chgrp '$l_sgroup' '$l_file'

fi [-n '$l_out2'] && l_output2='$l_output2

- File: 'l_file'l_out2'

done <<< '$(printf '%s ' '${a_skarr[@]}')'

```
else l_output=' - openSSH keys not found on the system'
fi unset a_skarr if [ -z '$l_output2' ]; then echo -e '
- No access changes required '
else echo -e '
- Remediation results:
$l_output2 '
fi }
```

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$ timeout: 7200

Hosts

10.74.6.135

```
The command script with multiple lines returned :

/bin/bash: line 19: & 0177 : syntax error: operand expected (error token is "& 0177 ")
```

4.2.4 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.

Rationale:

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 parameter above any Include entries as follows:

AllowUsers <userlist>

-OR- AllowGroups <grouplist>

-OR- DenyUsers <userlist>

-OR- DenyGroups <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 a file in Include location. If the Include location is not the default, /etc/ssh/sshd_config.d/*.conf, the audit will need to be modified to account for the Include location used.

Default Value:

None

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
FAILED - Config file exist and is configured correctly
File permission denied: /etc/ssh/sshd_config

-------------------------
FAILED - sshd access is configured
The command script with multiple lines returned :

/etc/ssh/sshd_config: Permission denied
port 22:
Fail
```

4.2.5 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.

Rationale:

Banners are used to warn connecting users of the particular site's policy regarding connection. Presenting a warning message prior to the normal user login may assist the prosecution of trespassers on the computer system.

Solution

Edit the /etc/ssh/sshd_config file to set the parameter above any Include 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.

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.9
800-53	AC-8
800-53R5	AC-8
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	AC-8
LEVEL	1A
NESA	M1.3.6
TBA-FIISB	45.2.4

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Pass$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

/etc/ssh/sshd_config: Permission denied
port 22:
Fail
```

4.2.7 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.

Rationale:

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 parameters above any Include 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.

Default Value:

ClientAliveInterval 0

ClientAliveCountMax 3

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.11
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)
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(iii)
ITSG-33	AC-12
LEVEL	1A
NIAV2	NS49

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

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

/etc/ssh/sshd_config: Permission denied
port 22:
Fail

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

/etc/ssh/sshd_config: Permission denied
port 22:
Fail

-------------------------
FAILED - ClientAliveCountMax configuration does not equal 0
File permission denied: /etc/ssh/sshd_config
```

4.2.9 Ensure sshd HostbasedAuthentication is disabled

Info

The HostbasedAuthentication parameter specifies if authentication is allowed through trusted hosts via the user of .rhosts, or /etc/hosts.equiv, along with successful public key client host authentication.

Rationale:

Even though the .rhosts files are ineffective if support is disabled in /etc/pam.conf, disabling the ability to use .rhosts files in SSH provides an additional layer of protection.

Solution

Edit the /etc/ssh/sshd_config file to set the parameter above any Include 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.

Default Value:

HostbasedAuthentication no

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.6
800-171	3.4.7
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
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
PASSED - sshd hostbasedauthentication setting
The command script with multiple lines returned :

/etc/ssh/sshd_config: Permission denied
port 22:
Pass

-------------------------
FAILED - config file HostbasedAuthentication setting
File permission denied: /etc/ssh/sshd_config
```

4.2.10 Ensure sshd IgnoreRhosts is enabled

Info

The IgnoreRhosts parameter specifies that .rhosts and .shosts files will not be used in RhostsRSAAuthentication or HostbasedAuthentication.

Rationale:

Setting this parameter forces users to enter a password when authenticating with SSH.

Solution

Edit the /etc/ssh/sshd_config file to set the parameter above any Include 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.

Default Value:

IgnoreRhosts yes

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
FAILED - config file IgnoreRhosts setting
File permission denied: /etc/ssh/sshd_config

-------------------------
PASSED - sshd ignorerhosts setting
The command script with multiple lines returned :

/etc/ssh/sshd_config: Permission denied
port 22:
Pass
```

4.2.12 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.

Rationale:

Setting the LoginGraceTime parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. It will also limit the number of concurrent unauthenticated connections While the recommended setting is 60 seconds (1 Minute), set the number based on site policy.

Solution

Edit the /etc/ssh/sshd_config file to set the parameter above any Include entries as follows:

LoginGraceTime 60

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.

Default Value:

LoginGraceTime 120

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-53	AC-10
800-53R5	AC-10
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
FAILED - sshd logingracetime setting
The command script with multiple lines returned :

/etc/ssh/sshd_config: Permission denied
port 22:
Fail

-------------------------
FAILED - config file logingracetime setting
File permission denied: /etc/ssh/sshd_config
```

4.2.13 Ensure sshd LogLevel is configured

Info

LogLevel gives the verbosity level that is used when logging messages from sshd. The possible values are: QUIET, FATAL, ERROR, INFO, VERBOSE, DEBUG, DEBUG1, DEBUG2, and DEBUG3. The default is INFO. DEBUG and DEBUG1 are equivalent. DEBUG2 and DEBUG3 each specify higher levels of debugging output.

Note: Logging with a DEBUG level violates the privacy of users and is not recommended.

Rationale:

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 parameter above any Include entries as follows:

LogLevel VERBOSE

-OR-

LogLevel INFO

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.

Default Value:

LogLevel INFO

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

------------------------
FAILED - sshd loglevel setting
The command script with multiple lines returned :

/etc/ssh/sshd_config: Permission denied
port 22:
Fail

------------------------
FAILED - config file loglevel setting
File permission denied: /etc/ssh/sshd_config
```

4.2.15 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.

Rationale:

Setting the MaxAuthTries parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, set the number based on site policy.

Solution

Edit the /etc/ssh/sshd_config file to set the parameter above any Include entries as follows:

MaxAuthTries 4

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.

Default Value:

MaxAuthTries 6

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

------------------------
FAILED - sshd maxauthtries setting
The command script with multiple lines returned :

/etc/ssh/sshd_config: Permission denied
port 22:
Fail

------------------------
FAILED - config file maxauthtries setting
File permission denied: /etc/ssh/sshd_config
```

4.2.16 Ensure sshd MaxSessions is configured

Info

The MaxSessions parameter specifies the maximum number of open sessions permitted from a given connection.

Rationale:

To protect a system from denial of service due to a large number of concurrent sessions, use the rate limiting function of MaxSessions to protect availability of sshd logins and prevent overwhelming the daemon.

Solution

Edit the /etc/ssh/sshd_config file to set the parameter above any Include entries as follows:

MaxSessions 10

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.

Default Value:

MaxSessions 10

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-53	AC-10
800-53R5	AC-10
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
FAILED - config file MaxSessions setting
File permission denied: /etc/ssh/sshd_config

-------------------------
FAILED - sshd maxsessions setting
The command script with multiple lines returned :

/etc/ssh/sshd_config: Permission denied
port 22:
Fail
```

4.2.17 Ensure sshd MaxStartups is configured

Info

The MaxStartups parameter specifies the maximum number of concurrent unauthenticated connections to the SSH daemon.

Rationale:

To protect a system from denial of service due to a large number of pending authentication connection attempts, use the rate limiting function of MaxStartups to protect availability of sshd logins and prevent overwhelming the daemon.

Solution

Edit the /etc/ssh/sshd_config file to set the parameter 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.

Default Value:

MaxStartups 10:30:100

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	CM-1
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	5.1
CSCV8	4.1
CSF	DE.AE-1
CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.DS-7
CSF	PR.IP-1
CSF	PR.IP-2
CSF	PR.IP-3
CSF	PR.PT-3
GDPR	32.1.b
GDPR	32.4
HIPAA	164.306(a)(1)
ITSG-33	CM-1
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	M1.2.2
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	GS8b
NIAV2	SS3
NIAV2	SS15a
NIAV2	SS16
NIAV2	VL2
NIAV2	VL7a
NIAV2	VL7b
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
QCSC-V1	7.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
FAILED - sshd maxstartups setting
The command script with multiple lines returned :

/etc/ssh/sshd_config: Permission denied
port 22:
Fail

-------------------------
FAILED - config file maxstartups setting
File permission denied: /etc/ssh/sshd_config
```

4.2.18 Ensure sshd PermitEmptyPasswords is disabled

Info

The PermitEmptyPasswords parameter specifies if the SSH server allows login to accounts with empty password strings.

Rationale:

Disallowing remote shell access to accounts that have an empty password reduces the probability of unauthorized access to the system.

Solution

Edit the /etc/ssh/sshd_config file to set the parameter above any Include entries as follows:

PermitEmptyPasswords 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.

Default Value:

PermitEmptyPasswords no

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
FAILED - config file permitemptypasswords setting
File permission denied: /etc/ssh/sshd_config

-------------------------
PASSED - sshd permitemptypasswords setting
The command script with multiple lines returned :

/etc/ssh/sshd_config: Permission denied
port 22:
Pass
```

4.2.19 Ensure sshd PermitRootLogin is disabled

Info

The PermitRootLogin parameter specifies if the root user can log in using SSH. The default is prohibit-password.

Rationale:

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 parameter above any Include entries as follows:

PermitRootLogin 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.

Default Value:

PermitRootLogin without-password

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.5
800-171	3.1.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
PASSED - sshd permitrootlogin setting
The command script with multiple lines returned :

/etc/ssh/sshd_config: Permission denied
port 22:
Pass

-------------------------
FAILED - config file permitrootlogin setting
```

```
File permission denied: /etc/ssh/sshd_config
```

4.2.20 Ensure sshd PermitUserEnvironment is disabled

Info

The PermitUserEnvironment option allows users to present environment options to the SSH daemon.

Rationale:

Permitting users the ability to set environment variables through the SSH daemon could potentially allow users to bypass security controls (e.g. setting an execution path that has SSH executing trojan'd programs)

Solution

Edit the /etc/ssh/sshd_config file to set the parameter above any Include entries as follows:

PermitUserEnvironment no

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.

Default Value:

PermitUserEnvironment no

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.6
800-171	3.4.7
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
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

------------------------
FAILED - config file PermitUserEnvironment setting
File permission denied: /etc/ssh/sshd_config

------------------------
PASSED - sshd permituserenvironment setting
The command script with multiple lines returned :

/etc/ssh/sshd_config: Permission denied
port 22:
Pass
```

4.2.21 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.

Rationale:

When usePAM is set to yes, PAM runs through account and session types properly. This is important if you want to restrict access to services based off of IP, time or other factors of the account. Additionally, you can make sure users inherit certain environment variables on login or disallow access to the server

Solution

Edit the /etc/ssh/sshd_config file to set the parameter above any Include entries as follows:

UsePAM yes

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/15289

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

------------------------
FAILED - config file UsePAM setting
File permission denied: /etc/ssh/sshd_config

------------------------
PASSED - sshd usepam setting
The command script with multiple lines returned :

/etc/ssh/sshd_config: Permission denied
port 22:
Pass
```

4.3.2 Ensure sudo commands use pty

Info

sudo can be configured to run only from a pseudo terminal (pseudo-pty).

Rationale:

Attackers can run a malicious program using sudo which would fork a background process that remains even when the main program has finished executing.

Impact:

WARNING: Editing the sudo configuration incorrectly can cause sudo to stop functioning. Always use visudo to modify sudo configuration files.

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

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.

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.5
800-171	3.1.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: /bin/grep -s -P '^[\s]*Defaults[\s]+([^#]+,[\s]*)?use_pty' /etc/sudoers /etc/sudoers.d/* | /bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'

expect: ^pass$

Hosts

10.74.6.135

```
The command '/bin/grep -s -P '^[\s]*Defaults[\s]+([^#]+,[\s]*)?use_pty' /etc/sudoers /etc/sudoers.d/
* | /bin/awk '{print} END {if (NR != 0) print "pass" ; else print "fail"}'' returned :

fail
```

4.4.2.1 Ensure active authselect profile includes pam modules

Info

A custom profile can be created by copying and customizing one of the default profiles. The default profiles include: sssd, winbind, or the nis. This profile can then be customized to follow site specific requirements.

You can select a profile for the authselect utility for a specific host. The profile will be applied to every user logging into the host.

Rationale:

A custom profile is required to customize many of the pam options.

Modifications made to a default profile may be overwritten during an update.

When you deploy a profile, the profile is applied to every user logging into the given host

Impact:

If local site customizations have been made to the authselect template or files in /etc/pam.d these custom entries should be added to the newly created custom profile before it's applied to the system. Please note that the order within the pam stacks is important when adding these entries. Specifically for the password stack, the use_authtok option is important, and should appear on all modules except for the first entry.

Example:

password requisite pam_pwquality.so local_users_only #<-- Top of password stack, doesn't include use_authtok

password required pam_pwhistory.so use_authtok #<-- subsequent entry in password stack, includes use_authtok

Solution

Perform the following to create a custom authselect profile, with the modules covered in this Benchmark correctly included in the custom profile template files Run the following command to create a custom authselect profile:

authselect create-profile <custom-profile name> <options>

Example:

authselect create-profile custom-profile -b sssd

Run the following command to select a custom authselect profile:

authselect select custom/<CUSTOM PROFILE NAME> {with-<OPTIONS>} {--force}

Example:

authselect select custom/custom-profile --backup=PAM_CONFIG_BACKUP --force

Note:

The PAM and authselect packages must be versions pam-1.3.1-25 and authselect-1.2.6-1 or newer

The example is based on a custom profile built (copied) from the the SSSD default authselect profile.

The example does not include the symlink option for the PAM or Metadata files. This is due to the fact that by linking the PAM files future updates to authselect may overwrite local site customizations to the custom profile

The --backup=PAM_CONFIG_BACKUP option will create a backup of the current config. The backup will be stored at /var/lib/authselect/backups/PAM_CONFIG_BACKUP

The --force option will force the overwrite of the existing files and automatically backup system files before writing any change unless the --nobackup option is set.

On a new system where authselect has not been configured. In this case, the --force option will force the selected authselect profile to be active and overwrite the existing files with files generated from the selected authselect profile's templates

On an existing system with a custom configuration. The --force option may be used, but ensure that you note the backup location included as your custom files will be overwritten. This will allow you to review the changes and add any necessary customizations to the template files for the authselect profile. After updating the templates, run the command authselect apply-changes to add these custom entries to the files in /etc/pam.d/

- IF - you receive an error ending with a message similar to:

[error] Refusing to activate profile unless those changes are removed or overwrite is requested.

Some unexpected changes to the configuration were detected. Use 'select' command instead.

This error is caused when the previous configuration was not created by authselect but by other tool or by manual changes and the --force option will be required to enable the authselect profile.

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.11.2
800-171	3.11.3
800-171	3.12.2
800-53	CA-5
800-53	RA-1
800-53	RA-5
800-53R5	CA-5
800-53R5	RA-1
800-53R5	RA-5
CSCV7	16.7
CSCV8	16.2
CSF	DE.CM-8
CSF	DE.DP-4
CSF	DE.DP-5
CSF	ID.GV-1

CSF	ID.GV-3
CSF	ID.RA-1
CSF	PR.IP-12
CSF	RS.CO-3
CSF	RS.MI-3
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
ISO/IEC-27001	A.12.6.1
ITSG-33	CA-5
ITSG-33	RA-1
ITSG-33	RA-5
LEVEL	1A
NESA	M1.2.2
NESA	M5.4.1
NESA	T7.7.1
NIAV2	NS9
PCI-DSSV3.2.1	6.1
PCI-DSSV4.0	6.3
PCI-DSSV4.0	6.3.1
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	2.7

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

head: cannot open '/etc/authselect/authselect.conf' for reading: No such file or directory
grep: /usr/share/authselect/default//password-auth: No such file or directory
```

```
grep: /usr/share/authselect/default//password-auth: No such file or directory
grep: /usr/share/authselect/default//password-auth: No such file or directory
grep: /usr/share/authselect/default//password-auth: No such file or directory
grep: /usr/share/authselect/default//password-auth: No such file or directory
grep: /usr/share/authselect/default//password-auth: No such file or directory
grep: /usr/share/authselect/default//password-auth: No such file or directory
grep: /usr/share/authselect/default//password-auth: No such file or directory
grep: /usr/share/authselect/default//password-auth: No such file or directory
grep: /usr/share/authselect/default//system-auth: No such file or directory
grep: /usr/share/authselect/default//system-auth: No such file or directory
grep: /usr/share/authselect/default//system-auth: No such file or directory
grep: /usr/share/authselect/default//system-auth: No such file or directory
grep: /usr/share/authselect/default//system-auth: No such file or directory
grep: /usr/share/authselect/default//system-auth: No such file or directory
grep: /usr/share/authselect/default//system-auth: No such file or directory
grep: /usr/share/authselect/default//system-auth: No such file or directory
grep: /usr/share/authselect/default//system-auth: No such file or directory

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


  - auth stack "pam_faillock.so with preauth" line missing in: "/usr/share/authselect/default//
password-auth"
  - auth stack "pam_faillock.so with authfail" line missing in: "/usr/share/authselect/default//
password-auth"
  - account stack "pam_faillock.so" line missing in: "/usr/share/authselect/default//password-auth"

  - auth stack "pam_unix.so" line missing in: "/usr/share/authselect/default//password-auth"
  - account stack "pam_unix.so" line m [...]
```

4.4.2.2 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.

Rationale:

Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Solution

Run the following script to verify the pam_faillock.so lines exist in the profile templates:

#!/usr/bin/env bash

{ l_module_name='faillock'

l_pam_profile='$(head -1 /etc/authselect/authselect.conf)'

if grep -Pq -- '^custom/' <<< '$l_pam_profile'; then l_pam_profile_path='/etc/authselect/$l_pam_profile'

else l_pam_profile_path='/usr/share/authselect/default/$l_pam_profile'

fi grep -P -- 'bpam_$l_module_name.sob' '$l_pam_profile_path'/{password,system}-auth }

Example Output with a custom profile named 'custom-profile':

/etc/authselect/custom/custom-profile/password-auth:auth required pam_faillock.so preauth silent {include if 'with-faillock'} /etc/authselect/custom/custom-profile/password-auth:auth required pam_faillock.so authfail {include if 'with-faillock'} /etc/authselect/custom/custom-profile/password-auth:account required pam_faillock.so {include if 'with-faillock'}

/etc/authselect/custom/custom-profile/system-auth:auth required pam_faillock.so preauth silent {include if 'with-faillock'} /etc/authselect/custom/custom-profile/system-auth:auth required pam_faillock.so authfail {include if 'with-faillock'} /etc/authselect/custom/custom-profile/system-auth:account required pam_faillock.so {include if 'with-faillock'}

Note: The lines may not include {include if 'with-faillock'}

- IF - the lines shown above are not returned, refer to the Recommendation 'Ensure active authselect profile includes pam modules' to update the authselect profile template files to include the pam_faillock entries before continuing this remediation.

- IF - the lines include {include if 'with-faillock'}, run the following command to enable the authselect with-faillock feature and update the files in /etc/pam.d to include pam_faillock.so:

authselect enable-feature with-faillock

- IF - any of the pam_faillock lines exist without {include if 'with-faillock'}, run the following command to update the files in /etc/pam.d to include pam_faillock.so:

authselect apply-changes

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	CM-1
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	16.7
CSCV8	4.1
CSF	DE.AE-1
CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.DS-7
CSF	PR.IP-1
CSF	PR.IP-2
CSF	PR.IP-3
CSF	PR.PT-3
GDPR	32.1.b
GDPR	32.4
HIPAA	164.306(a)(1)
ITSG-33	CM-1

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	M1.2.2
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	GS8b
NIAV2	SS3
NIAV2	SS15a
NIAV2	SS16
NIAV2	VL2
NIAV2	VL7a
NIAV2	VL7b
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
QCSC-V1	7.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
FAILED - Ensure at least one file named /etc/pam.d/system-auth exists and matches pattern ^h*authh
+(required|requisite)h+([^#r
]+h+)?pam_faillock.soh+([^#r
]+h+)?preauthb
The file "/etc/pam.d/system-auth" does not contain "^\h*auth\h+(required|requisite)\h+([^#\r\n]+\h
+)?pam_faillock\.so\h+([^#\r\n]+\h+)?preauth\b"

-------------------------
FAILED - Ensure at least one file named /etc/pam.d/system-auth exists and matches pattern ^h*authh
+(required|requisite)h+([^#r
]+h+)?pam_faillock.soh+([^#r
]+h+)?authfailb
The file "/etc/pam.d/system-auth" does not contain "^\h*auth\h+(required|requisite)\h+([^#\r\n]+\h
+)?pam_faillock\.so\h+([^#\r\n]+\h+)?authfail\b"

-------------------------
FAILED - Ensure at least one file named /etc/pam.d/password-auth exists and matches pattern ^h*authh
+(required|requisite)h+([^#r
]+h+)?pam_faillock.soh+([^#r
]+h+)?preauthb
The file "/etc/pam.d/password-auth" does not contain "^\h*auth\h+(required|requisite)\h+([^#\r\n]+\h
+)?pam_faillock\.so\h+([^#\r\n]+\h+)?preauth\b"

-------------------------
FAILED - Ensure at least one file named /etc/pam.d/password-auth exists and matches pattern ^h*authh
+(required|requisite)h+([^#r
]+h+)?pam_faillock.soh+([^#r
]+h+)?authfailb
The file "/etc/pam.d/password-auth" does not contain "^\h*auth\h+(required|requisite)\h+([^#\r\n]+\h
+)?pam_faillock\.so\h+([^#\r\n]+\h+)?authfail\b"

-------------------------
FAILED - Ensure at least one file named /etc/pam.d/system-auth exists and matches pattern ^h*authh
+(required|requisite)h+([^#r
]+h+)?pam_faillock.soh+([^#r
]+h+)?preauthb
The file "/etc/pam.d/system-auth" does not contain "^\h*account\h+(required|requisite)\h+([^#\r\n]+
\h+)?pam_faillock\.so\b"

-------------------------
FAILED - Ensure at least one file named /etc/pam.d/password-auth exists and matches pattern
 ^h*accounth+(required|requisite)h+([^#r
]+h+)?pam_faillock.sob
The file "/etc/pam.d/password-auth" does not contain "^\h*account\h+(required|requisite)\h+([^#\r
 [...]
```

4.4.2.4 Ensure pam_pwhistory module is enabled

Info

The pam_history.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.

Rationale:

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.

Solution

Run the following script to verify the pam_pwhistory.so lines exist in the profile templates:

#!/usr/bin/env bash

{ l_module_name='pwhistory'

l_pam_profile='$(head -1 /etc/authselect/authselect.conf)'

if grep -Pq -- '^custom/' <<< '$l_pam_profile'; then l_pam_profile_path='/etc/authselect/$l_pam_profile'

else l_pam_profile_path='/usr/share/authselect/default/$l_pam_profile'

fi grep -P -- 'bpam_$l_module_name.sob' '$l_pam_profile_path'/{password,system}-auth }

Example Output with a custom profile named 'custom-profile':

/etc/authselect/custom/custom-profile/password-auth:password required pam_pwhistory.so use_authtok {include if 'with-pwhistory'}

/etc/authselect/custom/custom-profile/system-auth:password required pam_pwhistory.so use_authtok {include if 'with-pwhistory'}

Note: The lines may not include {include if 'with-pwhistory'}

- IF - the lines shown above are not returned, refer to the Recommendation 'Ensure active authselect profile includes pam modules' to update the authselect profile template files to include the pam_pwhistory entries before continuing this remediation.

- IF - the lines include {include if 'with-pwhistory'}, run the following command to enable the authselect with-pwhistory feature and update the files in /etc/pam.d to include pam_faillock.so:

authselect enable-feature with-pwhistory

- IF - any of the pam_pwhistory lines exist without {include if 'with-pwhistory'}, run the following command to update the files in /etc/pam.d to include pam_pwhistory.so:

authselect apply-changes

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
FAILED - Ensure at least one file named /etc/pam.d/password-auth exists and matches pattern (?
i)^h*passwordh+(requisite|required)h+pam_pwhistory.sob
The file "/etc/pam.d/password-auth" does not contain "(?i)^\h*password\h+(requisite|required)\h
+pam_pwhistory\.so\b"

-------------------------
PASSED - Ensure at least one file named /etc/pam.d/system-auth exists and matches pattern (?
i)^h*passwordh+(requisite|required)h+pam_pwhistory.sob
Compliant file(s):
      /etc/pam.d/system-auth - regex '(?i)^\h*password\h+(requisite|required)\h+pam_pwhistory\.so
\b' found - expect '(?i)^\h*password\h+(requisite|required)\h+pam_pwhistory\.so\b' found in the
 following lines:
          20: password    requisite                                     pam_pwhistory.so
 try_first_pass local_users_only enforce_for_root retry=3 remember=5
          21: password    requisite     pam_pwhistory.so debug use_authtok remember=5 retry=3
```

4.4.3.2.1 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.

Rationale:

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

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

Solution

Edit or add the following line in /etc/security/pwquality.conf to a value of 2 or more and meets local site policy:

difok = 2

Create or modify a file ending in .conf 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:

sed -ri 's/^s*difoks*=/# &/' /etc/security/pwquality.conf # printf '

%s' 'difok = 2' >> /etc/security/pwquality.conf.d/50-pwdifok.conf

Run the following script to remove setting difok on the pam_pwquality.so module in the PAM files:

#!/usr/bin/env bash

{ for l_pam_file in system-auth password-auth; do l_authselect_file='/etc/authselect/$(head -1 /etc/authselect/authselect.conf | grep 'custom/')/$l_pam_file'

sed -ri 's/(^s*passwords+(requisite|required|sufficient)s+pam_pwquality.so.*)(s+difoks*=s*S+)(.*$)/14/' '$l_authselect_file'

done authselect apply-changes }

Default Value:

difok = 1

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
FAILED - Ensure at least one file named /etc/security/pwquality.conf exists and matches difok
 pattern
No matching files were found
Less than 1 matches of regex found

-------------------------
PASSED - Verify that difok is not set, is 2 or more, and conforms to local site policy
No matching files were found
```

4.4.3.2.4 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.

Rationale:

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

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

Solution

Create or modify a file ending in .conf 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:

sed -ri 's/^s*maxrepeats*=/# &/' /etc/security/pwquality.conf # printf '

%s' 'maxrepeat = 3' >> /etc/security/pwquality.conf.d/50-pwrepeat.conf

Run the following script to remove setting maxrepeat on the pam_pwquality.so module in the PAM files:

#!/usr/bin/env bash

{ for l_pam_file in system-auth password-auth; do l_authselect_file='/etc/authselect/$(head -1 /etc/authselect/authselect.conf | grep 'custom/')/$l_pam_file'

sed -ri 's/(^s*passwords+(requisite|required|sufficient)s+pam_pwquality.so.*)(s+maxrepeats*=s*S+)(.*$)/14/' '$l_authselect_file'

done authselect apply-changes }

Default Value:

maxrepeat = 0

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4

CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
PASSED - Verify that maxrepeat is not set, is 3 or less, not 0, and conforms to local site policy
No matching files were found

-------------------------
FAILED - Ensure at least one file named /etc/security/pwquality.conf exists and matches maxrepeat
 pattern
No matching files were found
Less than 1 matches of regex found
```

4.4.3.2.5 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.

Rationale:

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

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

Solution

Create or modify a file ending in .conf 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:

sed -ri 's/^s*maxsequences*=/# &/' /etc/security/pwquality.conf # printf '

%s' 'maxsequence = 3' >> /etc/security/pwquality.conf.d/50-pwmaxsequence.conf

Run the following script to remove setting maxsequence on the pam_pwquality.so module in the PAM files:

#!/usr/bin/env bash

{ for l_pam_file in system-auth password-auth; do l_authselect_file='/etc/authselect/$(head -1 /etc/authselect/authselect.conf | grep 'custom/')/$l_pam_file'

sed -ri 's/(^s*passwords+(requisite|required|sufficient)s+pam_pwquality.so.*)(s+maxsequences*=s*S+)(.*$)/14/' '$l_authselect_file'

done authselect apply-changes }

Default Value:

maxsequence = 0

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-53	IA-5(1)

800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
FAILED - Ensure at least one file named /etc/security/pwquality.conf exists and matches maxsequence
 pattern
No matching files were found
Less than 1 matches of regex found

-------------------------
PASSED - Verify that maxsequence is not set, is 3 or less, not 0, and conforms to local site policy
No matching files were found
```

4.4.3.2.7 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.

Rationale:

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

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

Solution

Edit or add the following line in a *.conf file in /etc/security/pwquality.conf.d or in /etc/security/pwquality.conf:

Example:

printf '

%s ' 'enforce_for_root' >> /etc/security/pwquality.conf.d/50-pwroot.conf

Default Value:

disabled

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: (?i)^\h*enforce_for_root\b file: /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf min_occurrences: 1 regex: (?i)^\h*enforce_for_root\b string_required: NO

Hosts

10.74.6.135

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

4.4.3.3.1 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.

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

Rationale:

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

Edit or add the following line in /etc/security/pwhistory.conf:

remember = 24

Run the following script to remove the remember argument from the pam_pwhistory.so module in /etc/pam.d/system-auth and /etc/pam.d/password-auth:

#!/usr/bin/env bash

{ for l_pam_file in system-auth password-auth; do l_authselect_file='/etc/authselect/$(head -1 /etc/authselect/authselect.conf | grep 'custom/')/$l_pam_file'

sed -ri 's/(^s*passwords+(requisite|required|sufficient)s+pam_pwhistory.so.*)(s+remembers*=s*S+)(.*$)/14/' '$l_authselect_file'

done authselect apply-changes }

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)

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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
FAILED - Verify that the remember option is not set to less than 24 on the pam_pwhistory.so module
Non-compliant file(s):
      /etc/pam.d/system-auth - regex '(?i)^\h*password\h+(requisite|required|sufficient)\h
+pam_pwhistory\.so\h+([^#\r]+\h+)?remember=' found - expect '(?i)^\h*password\h+(requisite|required|
sufficient)\h+pam_pwhistory\.so\h+([^#\r]+\h+)?remember=(2[4-9]|[3-9][0-9]|[1-9][0-9]{2,})\b' not
 found in the following lines:
          20: password    requisite                                     pam_pwhistory.so
 try_first_pass local_users_only enforce_for_root retry=3 remember=5
          21: password    requisite     pam_pwhistory.so debug use_authtok remember=5 retry=3

-------------------------
FAILED - Ensure at least one file named /etc/security/pwhistory.conf exists and matches remember
 pattern
The file "/etc/security/pwhistory.conf" does not contain "(?i)^\h*remember\h*="
```

4.4.3.3.2 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

Rationale:

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

Edit or add the following line in /etc/security/pwhistory.conf:

enforce_for_root

Default Value:

disabled

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: (?i)^\h*enforce_for_root\b file: /etc/security/pwhistory.conf regex: (?i)^\h*enforce_for_root\b

Hosts

10.74.6.135

```
The file "/etc/security/pwhistory.conf" does not contain "(?i)^\h*enforce_for_root\b"
```

4.4.3.3.3 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

Rationale:

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

Solution

Run the following script to verify the active authselect profile includes use_authtok on the password stack's pam_pwhistory.so module lines:

#!/usr/bin/env bash

{ l_pam_profile='$(head -1 /etc/authselect/authselect.conf)'

if grep -Pq -- '^custom/' <<< '$l_pam_profile'; then l_pam_profile_path='/etc/authselect/$l_pam_profile'

else l_pam_profile_path='/usr/share/authselect/default/$l_pam_profile'

fi grep -P -- '^h*passwordh+(requisite|required|sufficient)h+pam_pwhistory.soh+([^# r]+h+)?use_authtokb' '$l_pam_profile_path'/{password,system}-auth }

Example output:

/etc/authselect/custom/custom-profile/password-auth:password required pam_pwhistory.so use_authtok

/etc/authselect/custom/custom-profile/system-auth:password required pam_pwhistory.so use_authtok

- IF - the output does not include use_authtok, run the following script:

#!/usr/bin/env bash

{ l_pam_profile='$(head -1 /etc/authselect/authselect.conf)'

if grep -Pq -- '^custom/' <<< '$l_pam_profile'; then l_pam_profile_path='/etc/authselect/$l_pam_profile'

else l_pam_profile_path='/usr/share/authselect/default/$l_pam_profile'

fi for l_authselect_file in '$l_pam_profile_path'/password-auth '$l_pam_profile_path'/system-auth; do if grep -Pq '^h*passwordh+([^# r]+)h+pam_pwhistory.soh+([^# r]+h+)?use_authtokb' '$l_authselect_file'; then echo '- 'use_authtok' is already set'

else echo '- 'use_authtok' is not set. Updating template'

sed -ri 's/(^s*passwords+(requisite|required|sufficient)s+pam_pwhistory.sos+.*)$/& use_authtok/g' '$l_authselect_file'

fi done }

Run the following command to update the password-auth and system-auth files in /etc/pam.d to include the use_authtok argument on the password stack's pam_pwhistory.so lines:

authselect apply-changes

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-171	3.13.16
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
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)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

------------------------
PASSED - Ensure at least one file named /etc/pam.d/system-auth exists and matches password pattern
Compliant file(s):
      /etc/pam.d/system-auth - regex '(?i)^\h*password\h+(requisite|required|sufficient)\h
+pam_pwhistory\.so(\h+[^#\n\r]+)?\h+use_authtok\b' found - expect '(?i)^\h*password\h+(requisite|
required|sufficient)\h+pam_pwhistory\.so(\h+[^#\n\r]+)?\h+use_authtok\b' found in the following
 lines:
          21: password    requisite     pam_pwhistory.so debug use_authtok remember=5 retry=3

------------------------
FAILED - Ensure at least one file named /etc/pam.d/password-auth exists and matches password pattern
The file "/etc/pam.d/password-auth" does not contain "(?i)^\h*password\h+(requisite|required|
sufficient)\h+pam_pwhistory\.so(\h+[^#\n\r]+)?\h+use_authtok\b"
```

4.4.3.4.2 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 sha512 hash algorithm to be used.

Rationale:

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 script to verify the active authselect profile doesn't include the remember argument on the pam_unix.so module lines:

#!/usr/bin/env bash

{ l_pam_profile='$(head -1 /etc/authselect/authselect.conf)'

if grep -Pq -- '^custom/' <<< '$l_pam_profile'; then l_pam_profile_path='/etc/authselect/$l_pam_profile'

else l_pam_profile_path='/usr/share/authselect/default/$l_pam_profile'

fi grep -P -- '^h*passwordh+([^# r]+h+)pam_unix.sob' '$l_pam_profile_path'/{password,system}-auth }

Output should be similar to:

/etc/authselect/custom/custom-profile/password-auth:password sufficient pam_unix.so sha512 shadow {if not 'without-nullok':nullok} use_authtok

/etc/authselect/custom/custom-profile/system-auth:password sufficient pam_unix.so sha512 shadow {if not 'without-nullok':nullok} use_authtok

- IF - any line includes remember=, run the following script to remove the remember= from the pam_unix.so lines in the active authselect profile password-auth and system-auth' templates:

#!/usr/bin/env bash

{ l_pam_profile='$(head -1 /etc/authselect/authselect.conf)'

if grep -Pq -- '^custom/' <<< '$l_pam_profile'; then l_pam_profile_path='/etc/authselect/$l_pam_profile'

else l_pam_profile_path='/usr/share/authselect/default/$l_pam_profile'

fi for l_authselect_file in '$l_pam_profile_path'/password-auth '$l_pam_profile_path'/system-auth; do sed -ri 's/(^s*passwords+(requisite|required|sufficient)s+pam_unix.sos+.*)(remember=[1-9][0-9]*)(s*.*)$/14/g' '$l_authselect_file'

done }

Run the following command to update the password-auth and system-authfiles in/etc/pam.d to include pam_unix.so without the remember argument:

authselect apply-changes

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
FAILED - Ensure no file named /etc/pam.d/password-auth pam_unix.so contains remember
Non-compliant file(s):
      /etc/pam.d/password-auth - regex '(?i)^\h*password\h+([^#\n\r]+\h+)?pam_unix\.so\h+([^#\n\r]+
\h+)?remember*\b' found - expect '(?i)^\h*password\h+([^#\n\r]+\h+)?pam_unix\.so\h+([^#\n\r]+\h+)?
remember*\b' found in the following lines:
          20: password    sufficient                                    pam_unix.so sha512 shadow
 try_first_pass use_authtok remember=5

-------------------------
FAILED - Ensure no file named /etc/pam.d/system-auth pam_unix.so contains remember
Non-compliant file(s):
```

```
      /etc/pam.d/system-auth - regex '(?i)^\h*password\h+([^#\n\r]+\h+)?pam_unix\.so\h+([^#\n\r]+
\h+)?remember*\b' found - expect '(?i)^\h*password\h+([^#\n\r]+\h+)?pam_unix\.so\h+([^#\n\r]+\h+)?
remember*\b' found in the following lines:
          22: password    sufficient                                    pam_unix.so sha512 shadow
 try_first_pass use_authtok remember=5
```

4.5.1.4 Ensure inactive password lock is 30 days or less

Info

User accounts that have been inactive for over a given period of time can be automatically disabled. It is recommended that accounts that are inactive for 30 days after password expiration be disabled.

Rationale:

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 30 days:

useradd -D -f 30

Modify user parameters for all users with a password set to match:

chage --inactive 30 <user>

Default Value:

INACTIVE=-1

Additional Information:

A value of -1 would disable this setting.

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2

QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

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

INACTIVE=-1

-------------------------
PASSED - Users
The command '/bin/awk -F: '$1 !~ /#/ && $2 ~ /^[^!*]*$/ && ($7 == "" || $7 < 0 || $7 > 30) {print
 $1":"$7}' /etc/shadow | /bin/awk '{ print } END { if (NR == 0) print "pass" }'' returned :

awk: fatal: cannot open file `/etc/shadow' for reading (Permission denied)
pass
```

4.5.2.2 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

Rationale:

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.

Default Value:

System default umask

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: (?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))) file: /root/.bash_profile /root/.bashrc regex: (?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)))

Hosts

10.74.6.135

```
No files found: /root/.bash_profile /root/.bashrc
```

4.5.2.4 Ensure root password is set

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.

Rationale:

Access to root should be secured at all times.

Impact:

If there are any automated processes that relies on access to the root account without authentication, they will fail after remediation.

Solution

Set the root password with:

passwd root

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: /bin/passwd -S root expect: Password set

Hosts

10.74.6.135

```
The command '/bin/passwd -S root' returned :

Only root can do that.
```

5.1.1.5 Ensure logging is configured

Info

The /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files specifies rules for logging and which files are to be used to log certain classes of messages.

Rationale:

A great deal of important security-related information is sent via rsyslog (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Solution

Edit the following lines in the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files as appropriate for your environment.

Note: The below configuration is shown for example purposes only. Due care should be given to how the organization wish 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 restart rsyslog

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
PASSED - 'mail.err /var/log/mail.err'
Compliant file(s):
      /etc/rsyslog.conf - regex '^[\s]*mail\.err' found - expect 'mail\.err[\s]+/var/log/
mail.err[\s]*$' found in the following lines:
          109: mail.err                                                 /var/log/mail.err
          116: mail.err                                                 /var/log/mail.err
      /etc/rsyslog.d/siem.conf - regex not found

-------------------------
PASSED - 'local6,local7.* -/var/log/localmessages'
Compliant file(s):
      /etc/rsyslog.conf - regex '^[\s]*local6,local7' found - expect 'local6,local7\.\*[\s]+-/var/
log/localmessages[\s]*$' found in the following lines:
          60: local6,local7.*                                           -/var/log/localmessages
          82: local6,local7.*                                           -/var/log/localmessages
      /etc/rsyslog.d/siem.conf - regex not found

-------------------------
FAILED - 'auth,authpriv.* /var/log/secure'
Non-compliant file(s):
      /etc/rsyslog.conf - regex '^[\s]*auth,authpriv\.\*' found - expect 'auth,authpriv\.\*[\s]+/
var/log/secure[\s]*$' found in the following lines:
          53: auth,authpriv.*                                            /var/log/secure
      /etc/rsyslog.conf - regex '^[\s]*auth,authpriv\.\*' found - expect 'auth,authpriv\.\*[\s]+/
var/log/secure[\s]*$' not found in the following lines:
          75: auth,authpriv.*                                           -/var/log/secure

-------------------------
PASSED - 'local2,local3.* -/var/log/localmessages'
Compliant file(s):
      /etc/rsyslog.conf - regex '^[\s]*local2,local3' found - expect 'local2,local3\.\*[\s]+-/var/
log/localmessages[\s]*$' found in the following lines:
          58: local2,local3.*                                           -/var/log/localmessages
          80: local2,local3.*                                           -/var/log/localmessages
      /etc/rsyslog.d/siem.conf - regex not  [...]
```

5.1.4 Ensure all logfiles have appropriate access configured

Info

Log files stored in /var/log/ contain logged information from many services on the system and potentially from other logged hosts as well.

Rationale:

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 is captured in the event that the remediation causes issues.

#!/usr/bin/env bash

{ l_op2='' l_output2=''

l_uidmin='$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)'

file_test_fix() { l_op2=''

l_fuser='root'

l_fgroup='root'

if [$(($l_mode & $perm_mask)) -gt 0]; then l_op2='$l_op2

- Mode: '$l_mode' should be '$maxperm' or more restrictive

- Removing excess permissions'

chmod '$l_rperms' '$l_fname'

fi if [[! '$l_user' =~ $l_auser]]; then l_op2='$l_op2

- Owned by: '$l_user' and should be owned by '${l_auser//|/ or }'

- Changing ownership to: '$l_fuser''

chown '$l_fuser' '$l_fname'

fi if [[! '$l_group' =~ $l_agroup]]; then l_op2='$l_op2

- Group owned by: '$l_group' and should be group owned by '${l_agroup//|/ or }'

- Changing group ownership to: '$l_fgroup''

chgrp '$l_fgroup' '$l_fname'

fi [-n '$l_op2'] && l_output2='$l_output2

- File: '$l_fname' is:$l_op2 '

} unset a_file && a_file=() # clear and initialize array # Loop to create array with stat of files that could possibly fail one of the audits while IFS= read -r -d $'0' l_file; do [-e '$l_file'] && a_file+=('$(stat -Lc '%n^ %#a^%U^%u^%G^%g' '$l_file')') done < <(find -L /var/log -type f (-perm /0137 -o ! -user root -o ! -group root) -print0) while IFS='^' read -r l_fname l_mode l_user l_uid l_group l_gid; do l_bname='$(basename '$l_fname')'

```
case '$l_bname' in lastlog | lastlog.* | wtmp | wtmp.* | wtmp-* | btmp | btmp.* | btmp-* | README)
perm_mask='0113'
maxperm='$( printf '%o' $(( 0777 & ~$perm_mask)) )'
l_rperms='ug-x,o-wx'
l_auser='root'
l_agroup='(root|utmp)'
file_test_fix ;;
secure | auth.log | syslog | messages) perm_mask='0137'
maxperm='$( printf '%o' $(( 0777 & ~$perm_mask)) )'
l_rperms='u-x,g-wx,o-rwx'
l_auser='(root|syslog)'
l_agroup='(root|adm)'
file_test_fix ;;
SSSD | sssd) perm_mask='0117'
maxperm='$( printf '%o' $(( 0777 & ~$perm_mask)) )'
l_rperms='ug-x,o-rwx'
l_auser='(root|SSSD)'
l_agroup='(root|SSSD)'
file_test_fix ;;
gdm | gdm3) perm_mask='0117'
l_rperms='ug-x,o-rwx'
maxperm='$( printf '%o' $(( 0777 & ~$perm_mask)) )'
l_auser='root'
l_agroup='(root|gdm|gdm3)'
file_test_fix ;;
*.journal | *.journal~) perm_mask='0137'
maxperm='$( printf '%o' $(( 0777 & ~$perm_mask)) )'
l_rperms='u-x,g-wx,o-rwx'
l_auser='root'
l_agroup='(root|systemd-journal)'
file_test_fix ;;
*) perm_mask='0137'
maxperm='$( printf '%o' $(( 0777 & ~$perm_mask)) )'
l_rperms='u-x,g-wx,o-rwx'
l_auser='(root|syslog)'
l_agroup='(root|adm)'
if [ '$l_uid' -lt '$l_uidmin' ] && [ -z '$(awk -v grp='$l_group' -F: '$1==grp {print $4}' /etc/group)' ]; then if [[ !
'$l_user' =~ $l_auser ]]; then l_auser='(root|syslog|$l_user)'
fi if [[ ! '$l_group' =~ $l_agroup ]]; then l_tst=''
while l_out3='' read -r l_duid; do [ '$l_duid' -ge '$l_uidmin' ] && l_tst=failed done <<< '$(awk -F:
'$4=='$l_gid'' {print $3}' /etc/passwd)'
```

['$l_tst' != 'failed'] && l_agroup='(root|adm|$l_group)'

fi fi file_test_fix ;;

esac done <<< '$(printf '%s ' '${a_file[@]}')'

unset a_file # Clear array # If all files passed, then we report no changes if [-z '$l_output2']; then echo -e '- All files in '/var/log/' have appropriate permissions and ownership

- No changes required '

else # print report of changes echo -e '

$l_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 access configured.

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$ timeout: 7200

Hosts

10.74.6.135

```
The command script with multiple lines returned :

find: '/var/log/audit': Permission denied
find: '/var/log/aide': Permission denied
find: '/var/log/private': Permission denied
find: '/var/log/samba': Permission denied
find: '/var/log/sssd': Permission denied
find: '/var/log/filebeat': Permission denied
find: '/var/log/chrony': Permission denied
find: '/var/log/leapp': Permission denied

- Audit Results:
 ** Fail **

 - File: "/var/log/nginx/ebill_access_log-20230811.gz" is:
  - Owned by: "nginx" and should be owned by "(root or syslog)"

 - File: "/var/log/nginx/mba_access_log" is:
  - Owned by: "nginx" and should be owned by "(root or syslog)"

 - File: "/var/log/nginx/ebill_access_log-20230713.gz" is:
  - Owned by: "nginx" and should be owned by "(root or syslog)"

 - File: "/var/log/nginx/cdt-admin_access_log-20230811.gz" is:
  - Owned by: "nginx" and should be owned by "(root or syslog)"

 - File: "/var/log/nginx/fleetmanagement_access_log-20240602.gz" is:
  - Owned by: "nginx" and should be owned by "(root or syslog)"

 - File: "/var/log/nginx/internet_access_log" is:
  - Owned by: "nginx" and should be owned by "(root or syslog)"

 - File: "/var/log/nginx/internet_error_log" is:
  - Owned by: "nginx" and should be owned by "(root or syslog)"

 - File: "/var/log/nginx/sdm-viewer_access_log-20240603" is:
  - Owned by: "nginx" and should be owned by "(root or syslog)"

 - File: "/var/log/nginx/ebill_access_log-20230719.gz" is:
  - Owned by: "nginx" and should be owned by "(root or syslog)"

 - File: "/var/log/nginx/cdt-admin_access_log-20230724.gz" is:
  - Owned by: "nginx" and should be owned by "(root or syslog)"

 - File: "/var/log/nginx/cdt-admin_access_log-20230710.gz" is:
```

```
  - Owned by: "nginx" and should be owned by "(root or syslog)"

- File: "/var/log/nginx/cdt-admin_access_log-20230714.gz" is:
  - Owned by: "nginx" and should be owned by "(root or syslog)"

- File: "/var/log/nginx/cdt-admin_error_log-20230422.gz" is:
  - Owned by: "nginx" and should be owned by "(root or syslog)"

- File: "/var/l [...]
```

5.3.2 Ensure filesystem integrity is regularly checked

Info

Periodic checking of the filesystem integrity is needed to detect changes to the filesystem.

Rationale:

Periodic file checking allows the system administrator to determine on a regular basis if critical files have been changed in an unauthorized fashion.

Solution

- IF - cron will be used to schedule and run aide check Run the following command:

crontab -u root -e

Add the following line to the crontab:

0 5 * * * /usr/sbin/aide --check

- OR -

- IF - aidecheck.service and aidecheck.timer will be used to schedule and run aide check:

Create or edit the file /etc/systemd/system/aidecheck.service and add the following lines:

[Unit] Description=Aide Check

[Service] Type=simple ExecStart=/usr/sbin/aide --check

[Install] WantedBy=multi-user.target

Create or edit the file /etc/systemd/system/aidecheck.timer and add the following lines:

[Unit] Description=Aide check every day at 5AM

[Timer] OnCalendar=*-*-* 05:00:00 Unit=aidecheck.service

[Install] WantedBy=multi-user.target

Run the following commands:

chown root:root /etc/systemd/system/aidecheck.* # chmod 0644 /etc/systemd/system/aidecheck.*

systemctl daemon-reload

systemctl enable aidecheck.service # systemctl --now enable aidecheck.timer

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.7

800-171	3.3.1
800-171	3.3.2
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
FAILED - systemctl is-enabled aidecheck.timer
The command '/bin/systemctl is-enabled aidecheck.timer | /bin/awk '{print} END {if(NR==0) print
 "disabled" }'' returned :

Failed to get unit file state for aidecheck.timer: No such file or directory
disabled

-------------------------
FAILED - systemctl is-enabled aidecheck.service
The command '/bin/systemctl is-enabled aidecheck.service | /bin/awk '{print} END {if(NR==0) print
 "disabled" }'' returned :

Failed to get unit file state for aidecheck.service: No such file or directory
disabled

-------------------------
FAILED - systemctl status aidecheck.timer
The command '/bin/systemctl status aidecheck.timer' returned :

Unit aidecheck.timer could not be found.
```

5.3.3 Ensure cryptographic mechanisms are used to protect the integrity of audit tools

Info

Audit tools include, but are not limited to, vendor-provided and open source audit tools needed to successfully view and manipulate audit information system activity and records. Audit tools include custom queries and report generators.

Rationale:

Protecting the integrity of the tools used for auditing purposes is a critical step toward ensuring the integrity of audit information. Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Attackers may replace the audit tools or inject code into the existing tools with the purpose of providing the capability to hide or erase system activity from the audit logs.

Audit tools should be cryptographically signed in order to provide the capability to identify when the audit tools have been modified, manipulated, or replaced. An example is a checksum hash of the file or files.

Solution

Add or update the following selection lines for to a file ending in .conf in the /etc/aide.conf.d/ directory or to /etc/aide.conf to protect the integrity of the audit tools:

Audit Tools /sbin/auditctl p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/auditd p+i+n+u+g+s+b+acl+xattrs +sha512 /sbin/ausearch p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/aureport p+i+n+u+g+s+b+acl+xattrs +sha512 /sbin/autrace p+i+n+u+g+s+b+acl+xattrs+sha512 /sbin/augenrules p+i+n+u+g+s+b+acl+xattrs +sha512

MITRE ATT&CK Mappings:

Techniques / Sub-techniques

Tactics

Mitigations

T1070, T1070.002, T1083, T1083.000

TA0007

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-53	SI-7
800-53R5	SI-7
CSF	PR.DS-6
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(c)(1)
HIPAA	164.312(c)(2)
HIPAA	164.312(e)(2)(i)
ITSG-33	SI-7
ITSG-33	SI-7a.
LEVEL	1A
NESA	T3.4.1
NESA	T7.3.2
NESA	T7.3.3
PCI-DSSV3.2.1	10.5.5
QCSC-V1	3.2

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

FAILED

Hosts

10.74.6.135

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

-------------------------
FAILED - autrace
No matching files were found
Less than 1 matches of regex found

-------------------------
FAILED - augenrules
No matching files were found
Less than 1 matches of regex found

-------------------------
FAILED - auditd
No matching files were found
Less than 1 matches of regex found

-------------------------
FAILED - ausearch
No matching files were found
Less than 1 matches of regex found

-------------------------
FAILED - auditctl
No matching files were found
Less than 1 matches of regex found

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

6.1.12 Ensure no unowned or ungrouped files or directories 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.

Rationale:

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

name: find_orphan_files timeout: 7200

Hosts

10.74.6.135

```
The following 9 files are orphaned:

  /home/devepati
     owner: 815, group: staff, permissions: 0700

  /home/blksec
     owner: 451000101, group: 451000101, permissions: 0700

  /home/ericsson_anabi
     owner: 451000194, group: 451000194, permissions: 0700

  /home/ericsson_mislam
     owner: 451000203, group: 451000203, permissions: 0700

  /home/ericsson_jkalam
     owner: 451000197, group: 451000197, permissions: 0700

  /home/ericsson_niqbal
     owner: 451000184, group: 451000184, permissions: 0700

  /home/ericsson_psarker
     owner: 451000275, group: 451000275, permissions: 0700

  /home/ericsson_mrashid
     owner: 451000250, group: 451000250, permissions: 0700

  /var/spool/mail/devepati
     owner: 815, group: mail, permissions: 0660
```

Compliance 'SKIPPED'

Compliance 'PASSED'

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.

Rationale:

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 disable the freevxfs module:

-IF- the module is available in the running kernel:

Create a file ending in .conf with install freevxfs /bin/false in the /etc/modprobe.d/ directory

Create a file ending in .conf with blacklist freevxfs in the /etc/modprobe.d/ directory

Unload freevxfs from the kernel

-IF- available in ANY installed kernel:

Create a file ending in .conf with blacklist freevxfs in the /etc/modprobe.d/ directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

No remediation is necessary

#!/usr/bin/env bash

{ l_mname='freevxfs' # set module name l_mtype='fs' # set module type l_mpath='/lib/modules/**/kernel/$l_mtype'

l_mpname='$(tr '-' '_' <<< '$l_mname')'

l_mndir='$(tr '-' '/' <<< '$l_mname')'

module_loadable_fix() { # If the module is currently loadable, add 'install {MODULE_NAME} /bin/false' to a file in '/etc/modprobe.d'

l_loadable='$(modprobe -n -v '$l_mname')'

['$(wc -l <<< '$l_loadable')' -gt '1'] && l_loadable='$(grep -P -- '(^h*install|b$l_mname)b' <<< '$l_loadable')'

if ! grep -Pq -- '^h*install /bin/(true|false)' <<< '$l_loadable'; then echo -e '

- setting module: '$l_mname' to be not loadable'

echo -e 'install $l_mname /bin/false' >> /etc/modprobe.d/'$l_mpname'.conf fi } module_loaded_fix() { # If the module is currently loaded, unload the module if lsmod | grep '$l_mname' > /dev/null 2>&1; then echo -e '

- unloading module '$l_mname''

modprobe -r '$l_mname'

fi } module_deny_fix() { # If the module isn't deny listed, denylist the module if ! modprobe --showconfig | grep -Pq -- '^h*blacklisth+$l_mpnameb'; then echo -e '

- deny listing '$l_mname''

echo -e 'blacklist $l_mname' >> /etc/modprobe.d/'$l_mpname'.conf fi } # Check if the module exists on the system for l_mdir in $l_mpath; do if [-d '$l_mdir/$l_mndir'] && [-n '$(ls -A $l_mdir/$l_mndir)']; then echo -e '

- module: '$l_mname' exists in '$l_mdir'

- checking if disabled...'

module_deny_fix if ['$l_mdir' = '/lib/modules/$(uname -r)/kernel/$l_mtype']; then module_loadable_fix module_loaded_fix fi else echo -e '

- module: '$l_mname' doesn't exist in '$l_mdir'

'

fi done echo -e '

- remediation of module: '$l_mname' complete '

}

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **

 - module: "freevxfs" doesn't exist in "/lib/modules/4.18.0-513.24.1.el8_9.x86_64/kernel/fs"
 - module: "freevxfs" doesn't exist in "/lib/modules/5.4.17-2136.330.7.1.el8uek.x86_64/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.

Rationale:

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 disable the hfs module:

-IF- the module is available in the running kernel:

Create a file ending in .conf with install hfs /bin/false in the /etc/modprobe.d/ directory

Create a file ending in .conf with blacklist hfs in the /etc/modprobe.d/ directory

Unload hfs from the kernel

-IF- available in ANY installed kernel:

Create a file ending in .conf with blacklist hfs in the /etc/modprobe.d/ directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

No remediation is necessary

#!/usr/bin/env bash

{ l_mname='hfs' # set module name l_mtype='fs' # set module type l_mpath='/lib/modules/**/kernel/$l_mtype'

l_mpname='$(tr '-' '_' <<< '$l_mname')'

l_mndir='$(tr '-' '/' <<< '$l_mname')'

module_loadable_fix() { # If the module is currently loadable, add 'install {MODULE_NAME} /bin/false' to a file in '/etc/modprobe.d'

l_loadable='$(modprobe -n -v '$l_mname')'

['$(wc -l <<< '$l_loadable')' -gt '1'] && l_loadable='$(grep -P -- '(^h*install|b$l_mname)b' <<< '$l_loadable')'

if ! grep -Pq -- '^h*install /bin/(true|false)' <<< '$l_loadable'; then echo -e '

- setting module: '$l_mname' to be not loadable'

echo -e 'install $l_mname /bin/false' >> /etc/modprobe.d/'$l_mpname'.conf fi } module_loaded_fix() { # If the module is currently loaded, unload the module if lsmod | grep '$l_mname' > /dev/null 2>&1; then echo -e '

- unloading module '$l_mname''

modprobe -r '$l_mname'

fi } module_deny_fix() { # If the module isn't deny listed, denylist the module if ! modprobe --showconfig | grep -Pq -- '^h*blacklisth+$l_mpnameb'; then echo -e '

- deny listing '$l_mname''

echo -e 'blacklist $l_mname' >> /etc/modprobe.d/'$l_mpname'.conf fi } # Check if the module exists on the system for l_mdir in $l_mpath; do if [-d '$l_mdir/$l_mndir'] && [-n '$(ls -A $l_mdir/$l_mndir)']; then echo -e '

- module: '$l_mname' exists in '$l_mdir'

- checking if disabled...'

module_deny_fix if ['$l_mdir' = '/lib/modules/$(uname -r)/kernel/$l_mtype']; then module_loadable_fix module_loaded_fix fi else echo -e '

- module: '$l_mname' doesn't exist in '$l_mdir'

'

fi done echo -e '

- remediation of module: '$l_mname' complete '

}

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **

 - module: "hfs" doesn't exist in "/lib/modules/4.18.0-513.24.1.el8_9.x86_64/kernel/fs"
 - module: "hfs" doesn't exist in "/lib/modules/5.4.17-2136.330.7.1.el8uek.x86_64/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.

Rationale:

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 disable the hfsplus module:

-IF- the module is available in the running kernel:

Create a file ending in .conf with install hfsplus /bin/false in the /etc/modprobe.d/ directory

Create a file ending in .conf with blacklist hfsplus in the /etc/modprobe.d/ directory

Unload hfsplus from the kernel

-IF- available in ANY installed kernel:

Create a file ending in .conf with blacklist hfsplus in the /etc/modprobe.d/ directory

-IF- the kernel module is not available on the system or pre-compiled into the kernel:

No remediation is necessary

#!/usr/bin/env bash

{ l_mname='hfsplus' # set module name l_mtype='fs' # set module type l_mpath='/lib/modules/**/kernel/$l_mtype'

l_mpname='$(tr '-' '_' <<< '$l_mname')'

l_mndir='$(tr '-' '/' <<< '$l_mname')'

module_loadable_fix() { # If the module is currently loadable, add 'install {MODULE_NAME} /bin/false' to a file in '/etc/modprobe.d'

l_loadable='$(modprobe -n -v '$l_mname')'

['$(wc -l <<< '$l_loadable')' -gt '1'] && l_loadable='$(grep -P -- '(^h*install|b$l_mname)b' <<< '$l_loadable')'

if ! grep -Pq -- '^h*install /bin/(true|false)' <<< '$l_loadable'; then echo -e '

- setting module: '$l_mname' to be not loadable'

echo -e 'install $l_mname /bin/false' >> /etc/modprobe.d/'$l_mpname'.conf fi } module_loaded_fix() { # If the module is currently loaded, unload the module if lsmod | grep '$l_mname' > /dev/null 2>&1; then echo -e '

- unloading module '$l_mname''

modprobe -r '$l_mname'

fi } module_deny_fix() { # If the module isn't deny listed, denylist the module if ! modprobe --showconfig | grep -Pq -- '^h*blacklisth+$l_mpnameb'; then echo -e '

- deny listing '$l_mname''

echo -e 'blacklist $l_mname' >> /etc/modprobe.d/'$l_mpname'.conf fi } # Check if the module exists on the system for l_mdir in $l_mpath; do if [-d '$l_mdir/$l_mndir'] && [-n '$(ls -A $l_mdir/$l_mndir)']; then echo -e '

- module: '$l_mname' exists in '$l_mdir'

- checking if disabled...'

module_deny_fix if ['$l_mdir' = '/lib/modules/$(uname -r)/kernel/$l_mtype']; then module_loadable_fix module_loaded_fix fi else echo -e '

- module: '$l_mname' doesn't exist in '$l_mdir'

'

fi done echo -e '

- remediation of module: '$l_mname' complete '

}

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **

 - module: "hfsplus" doesn't exist in "/lib/modules/4.18.0-513.24.1.el8_9.x86_64/kernel/fs"
 - module: "hfsplus" doesn't exist in "/lib/modules/5.4.17-2136.330.7.1.el8uek.x86_64/kernel/fs"
```

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%.

Rationale:

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.

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.

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/tmptmpfs 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

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A

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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - mount check
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/tmp[\s]+' found - expect '[\s]+/tmp[\s]+' found in the
 following lines:
          30: 49 97 0:44 / /tmp rw,nosuid,nodev,noexec shared:30 - tmpfs tmpfs rw,seclabel

-------------------------
PASSED - config check
The command '/bin/systemctl is-enabled tmp.mount' returned :

enabled
```

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.

Rationale:

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/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2

SWIFT-CSCV1 2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: nodev file: /proc/self/mountinfo regex: [\s]+/tmp[\s]+ required: NO

Hosts

10.74.6.135

```
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/tmp[\s]+' found - expect 'nodev' found in the following
 lines:
          30: 49 97 0:44 / /tmp rw,nosuid,nodev,noexec shared:30 - tmpfs tmpfs rw,seclabel
```

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.

Rationale:

Since the /tmp filesystem is only intended for temporary file storage, set this option to ensure that users cannot create setuid files in /tmp.

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: nosuid file: /proc/self/mountinfo regex: [\s]+/tmp[\s]+ required: NO

Hosts

10.74.6.135

```
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/tmp[\s]+' found - expect 'nosuid' found in the following
 lines:
          30: 49 97 0:44 / /tmp rw,nosuid,nodev,noexec shared:30 - tmpfs tmpfs rw,seclabel
```

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.

Rationale:

Since the /tmp filesystem is only intended for temporary file storage, set this option to ensure that users cannot run executable binaries from /tmp.

Impact:

Setting the noexec option on /tmp may prevent installation and/or updating of some 3rd party software.

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

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: noexec file: /proc/self/mountinfo regex: [\s]+/tmp[\s]+ required: NO

Hosts

10.74.6.135

```
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/tmp[\s]+' found - expect 'noexec' found in the following
 lines:
          30: 49 97 0:44 / /tmp rw,nosuid,nodev,noexec shared:30 - tmpfs tmpfs rw,seclabel
```

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).

Rationale:

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.

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.

Solution

For specific configuration requirements of the /dev/shm mount for your environment, modify /etc/fstab.

Example:

tmpfs/dev/shmtmpfs defaults,rw,nosuid,nodev,noexec,relatime,size=2G 0 0

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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

GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: [\s]+/dev/shm[\s]+ file: /proc/self/mountinfo regex: [\s]+/dev/shm[\s]+ required: NO

Hosts

10.74.6.135

```
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/dev/shm[\s]+' found - expect '[\s]+/dev/shm[\s]+' found in
 the following lines:
          5: 26 24 0:22 / /dev/shm rw,nosuid,nodev,noexec shared:23 - tmpfs tmpfs rw,seclabel
```

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.

Rationale:

Since the /dev/shm filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create special devices in /dev/shm partitions.

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: nodev file: /proc/self/mountinfo regex: [\s]+/dev/shm[\s]+ required: NO

Hosts

10.74.6.135

```
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/dev/shm[\s]+' found - expect 'nodev' found in the
 following lines:
          5: 26 24 0:22 / /dev/shm rw,nosuid,nodev,noexec shared:23 - tmpfs tmpfs rw,seclabel
```

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.

Rationale:

Setting this option on a file system prevents users from introducing privileged programs onto the system and allowing non-root users to execute them.

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: nosuid file: /proc/self/mountinfo regex: [\s]+/dev/shm[\s]+ required: NO

Hosts

10.74.6.135

```
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/dev/shm[\s]+' found - expect 'nosuid' found in the
 following lines:
          5: 26 24 0:22 / /dev/shm rw,nosuid,nodev,noexec shared:23 - tmpfs tmpfs rw,seclabel
```

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.

Rationale:

Setting this option on a file system prevents users from executing programs from shared memory. This deters users from introducing potentially malicious software on the system.

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: noexec file: /proc/self/mountinfo regex: [\s]+/dev/shm[\s]+ required: NO

Hosts

10.74.6.135

```
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/dev/shm[\s]+' found - expect 'noexec' found in the
 following lines:
          5: 26 24 0:22 / /dev/shm rw,nosuid,nodev,noexec shared:23 - tmpfs tmpfs rw,seclabel
```

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.

Rationale:

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: nodev file: /proc/self/mountinfo regex: [\s]+/home[\s]+ required: NO

Hosts

10.74.6.135

```
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/home[\s]+' found - expect 'nodev' found in the following
 lines:
          33: 120 97 253:2 / /home rw,nosuid,nodev,relatime shared:65 - xfs /dev/mapper/vgData-
lv_home rw,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota
```

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.

Rationale:

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: nosuid file: /proc/self/mountinfo regex: [\s]+/home[\s]+ required: NO

Hosts

10.74.6.135

```
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/home[\s]+' found - expect 'nosuid' found in the following
 lines:
          33: 120 97 253:2 / /home rw,nosuid,nodev,relatime shared:65 - xfs /dev/mapper/vgData-
lv_home rw,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota
```

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.

Rationale:

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: nodev file: /proc/self/mountinfo regex: [\s]+/var[\s]+ required: NO

Hosts

10.74.6.135

```
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/var[\s]+' found - expect 'nodev' found in the following
 lines:
          36: 129 97 253:6 / /var rw,nosuid,nodev,relatime shared:71 - xfs /dev/mapper/vgData-lv_var
 rw,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota
```

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.

Rationale:

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: nosuid file: /proc/self/mountinfo regex: [\s]+/var[\s]+ required: NO

Hosts

10.74.6.135

```
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/var[\s]+' found - expect 'nosuid' found in the following
 lines:
          36: 129 97 253:6 / /var rw,nosuid,nodev,relatime shared:71 - xfs /dev/mapper/vgData-lv_var
 rw,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota
```

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.

Rationale:

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: nodev file: /proc/self/mountinfo regex: [\s]+/var/tmp[\s]+ required: NO

Hosts

10.74.6.135

```
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.

Rationale:

Since the /var/tmp filesystem is only intended for temporary file storage, set this option to ensure that users cannot create setuid files in /var/tmp.

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: nosuid file: /proc/self/mountinfo regex: [\s]+/var/tmp[\s]+ required: NO

Hosts

10.74.6.135

```
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.

Rationale:

Since the /var/tmp filesystem is only intended for temporary file storage, set this option to ensure that users cannot run executable binaries from /var/tmp.

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: noexec file: /proc/self/mountinfo regex: [\s]+/var/tmp[\s]+ required: NO

Hosts

10.74.6.135

```
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.

Rationale:

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: nodev file: /proc/self/mountinfo regex: [\s]+/var/log[\s]+ required: NO

Hosts

10.74.6.135

```
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/var/log[\s]+' found - expect 'nodev' found in the
 following lines:
          37: 132 129 253:5 / /var/log rw,nosuid,nodev,noexec,relatime shared:73 - xfs /dev/mapper/
vgData-lv_varlog rw,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota
```

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.

Rationale:

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: nosuid file: /proc/self/mountinfo regex: [\s]+/var/log[\s]+ required: NO

Hosts

10.74.6.135

```
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/var/log[\s]+' found - expect 'nosuid' found in the
 following lines:
          37: 132 129 253:5 / /var/log rw,nosuid,nodev,noexec,relatime shared:73 - xfs /dev/mapper/
vgData-lv_varlog rw,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota
```

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.

Rationale:

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: noexec file: /proc/self/mountinfo regex: [\s]+/var/log[\s]+ required: NO

Hosts

10.74.6.135

```
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/var/log[\s]+' found - expect 'noexec' found in the
 following lines:
          37: 132 129 253:5 / /var/log rw,nosuid,nodev,noexec,relatime shared:73 - xfs /dev/mapper/
vgData-lv_varlog rw,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota
```

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.

Rationale:

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: nodev file: /proc/self/mountinfo regex: [\s]+/var/log/audit[\s]+ required: NO

Hosts

10.74.6.135

```
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/var/log/audit[\s]+' found - expect 'nodev' found in the
 following lines:
          39: 138 132 253:7 / /var/log/audit rw,nosuid,nodev,noexec,relatime shared:77 - xfs /dev/
mapper/vgData-lv_varlogaudit rw,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota
```

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.

Rationale:

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: nosuid file: /proc/self/mountinfo regex: [\s]+/var/log/audit[\s]+ required: NO

Hosts

10.74.6.135

```
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/var/log/audit[\s]+' found - expect 'nosuid' found in the
 following lines:
          39: 138 132 253:7 / /var/log/audit rw,nosuid,nodev,noexec,relatime shared:77 - xfs /dev/
mapper/vgData-lv_varlogaudit rw,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota
```

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.

Rationale:

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: noexec file: /proc/self/mountinfo regex: [\s]+/var/log/audit[\s]+ required: NO

Hosts

10.74.6.135

```
Compliant file(s):
      /proc/self/mountinfo - regex '[\s]+/var/log/audit[\s]+' found - expect 'noexec' found in the
 following lines:
          39: 138 132 253:7 / /var/log/audit rw,nosuid,nodev,noexec,relatime shared:77 - xfs /dev/
mapper/vgData-lv_varlogaudit rw,seclabel,attr2,inode64,logbufs=8,logbsize=32k,noquota
```

1.3.2 Ensure permissions on bootloader config are configured

Info

The grub files contain information on boot settings and passwords for unlocking boot options.

Rationale:

Setting the permissions to read and write for root only prevents non-root users from seeing the boot parameters or changing them. Non-root users who read the boot parameters may be able to identify weaknesses in security upon boot and be able to exploit them.

Solution

Run the following to update the mode, ownership, and group ownership of the grub configuration files:

-IF- the system uses UEFI (Files located in /boot/efi/EFI/*) Edit /etc/fstab and add the fmask=0077, uid=0, and gid=0 options:

Example:

<device> /boot/efi vfat defaults,umask=0027,fmask=0077,uid=0,gid=0 0 0

Note: This may require a re-boot to enable the change

-OR-

-IF- the system uses BIOS (Files located in /boot/grub2/*) Run the following commands to set ownership and permissions on your grub configuration file(s):

[-f /boot/grub2/grub.cfg] && chown root:root /boot/grub2/grub.cfg # [-f /boot/grub2/grub.cfg] && chmod u-x,go-rwx /boot/grub2/grub.cfg

[-f /boot/grub2/grubenv] && chown root:root /boot/grub2/grubenv # [-f /boot/grub2/grubenv] && chmod u-x,go-rwx /boot/grub2/grubenv

[-f /boot/grub2/user.cfg] && chown root:root /boot/grub2/user.cfg # [-f /boot/grub2/user.cfg] && chmod u-x,go-rwx /boot/grub2/user.cfg

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$ timeout: 7200

Hosts

10.74.6.135

```
The command script with multiple lines returned :

find: '/boot/efi': Permission denied
find: '/boot/grub2': Permission denied
find: '/boot/loader/entries': Permission denied

- Audit Result:
  *** PASS ***
- * Correctly set * :
```

1.4.3 Ensure core dump backtraces are disabled

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.

Rationale:

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

Solution

Create or edit the file /etc/systemd/coredump.conf, or a file in the /etc/systemd/coredump.conf.d directory ending in .conf.

Edit or add the following line:

ProcessSizeMax=0

Default Value:

ProcessSizeMax=2G

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.6
800-171	3.4.7
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
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **

 - "ProcessSizeMax" is correctly set to "0" in "/etc/systemd/coredump.conf"
```

1.4.4 Ensure core dump storage is disabled

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.

Rationale:

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

Solution

Create or edit the file /etc/systemd/coredump.conf, or a file in the /etc/systemd/coredump.conf.d directory ending in .conf.

Edit or add the following line:

Storage=none

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.6
800-171	3.4.7
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
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **

 - "Storage" is correctly set to "none" in "/etc/systemd/coredump.conf"
```

1.5.1.1 Ensure SELinux is installed

Info

SELinux provides Mandatory Access Control.

Rationale:

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

Solution

Run the following command to install SELinux:

dnf install libselinux

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: gt required: YES rpm: libselinux-0.0.0-0

Hosts

10.74.6.135

```
The local RPM is newer than libselinux-0.0.0-0 (libselinux-2.9-8.el8)
```

1.5.1.2 Ensure SELinux is not disabled in bootloader configuration

Info

Configure SELINUX to be enabled at boot time and verify that it has not been overwritten by the grub boot parameters.

Rationale:

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

Impact:

Files created while SELinux is disabled are not labeled at all. This behavior causes problems when changing to enforcing mode because files are labeled incorrectly or are not labeled at all. To prevent incorrectly labeled and unlabeled files from causing problems, file systems are automatically relabeled when changing from the disabled state to permissive or enforcing mode. This can be a long running process that should be accounted for as it may extend downtime during initial re-boot.

Solution

Run the following command to remove the selinux=0 and enforcing=0 parameters:

grubby --update-kernel ALL --remove-args 'selinux=0 enforcing=0'

Run the following command to remove the selinux=0 and enforcing=0 parameters if they were created by the deprecated grub2-mkconfig command:

grep -Prsq -- 'h*([^# r]+h+)?kernelopts=([^# r]+h+)?(selinux|enforcing)=0b' /boot/grub2 /boot/efi && grub2-mkconfig -o '$(grep -Prl -- 'h*([^# r]+h+)?kernelopts=([^# r]+h+)?(selinux|enforcing)=0b' /boot/grub2 /boot/efi)'

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: /sbin/grubby --info=ALL | /bin/grep -Po '(selinux|enforcing)=0' | /bin/awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}'

expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command '/sbin/grubby --info=ALL | /bin/grep -Po '(selinux|enforcing)=0' | /bin/awk '{print} END
 {if (NR == 0) print "pass" ; else print "fail"}'' returned :

grep: /boot/grub2/grubenv: Permission denied
pass
```

1.5.1.3 Ensure SELinux policy is configured

Info

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

Rationale:

Security configuration requirements vary from site to site. Some sites may mandate a policy that is stricter than the default policy, which is perfectly acceptable. This item is intended to ensure that at least the default recommendations are met.

Solution

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

SELINUXTYPE=targeted

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - sestatus
The command '/sbin/sestatus' returned :

SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33

-------------------------
PASSED - /etc/selinux/config
Compliant file(s):
      /etc/selinux/config - regex '(?i)^[\s]*SELINUXTYPE[\s]*=' found - expect '(?
i)^[\s]*SELINUXTYPE[\s]*=[\s]*(targeted|mls)[\s]*$' found in the following lines:
          12: SELINUXTYPE=targeted
```

1.5.1.4 Ensure the SELinux mode is not disabled

Info

SELinux can run in one of three modes: disabled, permissive, or enforcing:

Enforcing - Is the default, and recommended, mode of operation; in enforcing mode SELinux operates normally, enforcing the loaded security policy on the entire system.

Permissive - The system acts as if SELinux is enforcing the loaded security policy, including labeling objects and emitting access denial entries in the logs, but it does not actually deny any operations. While not recommended for production systems, permissive mode can be helpful for SELinux policy development.

Disabled - Is strongly discouraged; not only does the system avoid enforcing the SELinux policy, it also avoids labeling any persistent objects such as files, making it difficult to enable SELinux in the future

Note: You can set individual domains to permissive mode while the system runs in enforcing mode. For example, to make the httpd_t domain permissive:

semanage permissive -a httpd_t

Rationale:

Running SELinux in disabled mode is strongly discouraged; not only does the system avoid enforcing the SELinux policy, it also avoids labeling any persistent objects such as files, making it difficult to enable SELinux in the future.

Solution

Run one of the following commands to set SELinux's running mode:

To set SELinux mode to Enforcing:

setenforce 1

-OR- To set SELinux mode to Permissive:

setenforce 0

Edit the /etc/selinux/config file to set the SELINUX parameter:

For Enforcing mode:

SELINUX=enforcing

-OR- For Permissive mode:

SELINUX=permissive

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - /etc/selinux/config
Compliant file(s):
```

```
      /etc/selinux/config - regex '(?i)^[\s]*SeLinux[\s]*=' found - expect '(?
i)^[\s]*SeLinux[\s]*=[\s]*(Enforcing|Permissive)[\s]*$' found in the following lines:
          7: SELINUX=enforcing

-------------------------
PASSED - getenforce
The command '/sbin/getenforce' returned :

Enforcing
```

1.5.1.7 Ensure the MCS Translation Service (mcstrans) is not installed

Info

The mcstransd daemon provides category label information to client processes requesting information. The label translations are defined in /etc/selinux/targeted/setrans.conf

Rationale:

Since this service is not used very often, remove it to reduce the amount of potentially vulnerable code running on the system.

Solution

Run the following command to uninstall mcstrans:

dnf remove mcstrans

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lt rpm: mcstrans-0.0.0-0

Hosts

10.74.6.135

```
The package 'mcstrans-0.0.0-0' is not installed
```

1.5.1.8 Ensure SETroubleshoot is not installed

Info

The SETroubleshoot service notifies desktop users of SELinux denials through a user-friendly interface. The service provides important information around configuration errors, unauthorized intrusions, and other potential errors.

Rationale:

The SETroubleshoot service is an unnecessary daemon to have running on a server, especially if X Windows is disabled.

Solution

Run the following command to uninstall setroubleshoot:

dnf remove setroubleshoot

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	14.6
CSCV8	4.8
CSF	PR.IP-1
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lt rpm: setroubleshoot-0.0.0-0

Hosts

10.74.6.135

```
The package 'setroubleshoot-0.0.0-0' is not installed
```

1.6.1 Ensure system wide crypto policy is not set to legacy

Info

When a system-wide policy is set up, the default behavior of applications will be to follow the policy. Applications will be unable to use algorithms and protocols that do not meet the policy, unless you explicitly request the application to do so.

The system-wide crypto-policies followed by the crypto core components allow consistently deprecating and disabling algorithms system-wide.

The LEGACY policy ensures maximum compatibility with version 5 of the operating system and earlier; it is less secure due to an increased attack surface. In addition to the DEFAULT level algorithms and protocols, it includes support for the TLS 1.0 and 1.1 protocols. The algorithms DSA, 3DES, and RC4 are allowed, while RSA keys and Diffie-Hellman parameters are accepted if they are at least 1023 bits long.

Rationale:

If the LEGACY system-wide crypto policy is selected, it includes support for TLS 1.0, TLS 1.1, and SSH2 protocols or later. The algorithms DSA, 3DES, and RC4 are allowed, while RSA and Diffie-Hellman parameters are accepted if larger than 1023-bits.

These legacy protocols and algorithms can make the system vulnerable to attacks, including those listed in RFC 7457

Impact:

Environments that require compatibility with older insecure protocols may require the use of the less secure LEGACY policy level.

Solution

Run the following command to change the system-wide crypto policy

update-crypto-policies --set <CRYPTO POLICY>

Example:

update-crypto-policies --set DEFAULT

Run the following to make the updated system-wide crypto policy active

update-crypto-policies

Default Value:

DEFAULT

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.13
800-171	3.5.2
800-171	3.13.8
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
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/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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: (?i)^[\s]*LEGACY[\s]*([\s]+#.*)?$ file: /etc/crypto-policies/config regex: (?i)^[\s]*LEGACY[\s]*([\s]+#.*)?$

Hosts

10.74.6.135

```
The file "/etc/crypto-policies/config" does not contain "(?i)^[\s]*LEGACY[\s]*([\s]+#.*)?$"
```

1.6.2 Ensure system wide crypto policy disables sha1 hash and signature support

Info

SHA-1 (Secure Hash Algorithm) is a cryptographic hash function that produces a 160 bit hash value.

Rationale:

The SHA-1 hash function has an inherently weak design, and advancing cryptanalysis has made it vulnerable to attacks. The most significant danger for a hash algorithm is when a 'collision' which happens when two different pieces of data produce the same hash value occurs. This hashing algorithm has been considered weak since 2005.

Note: The use of SHA-1 with hashbased message authentication codes (HMAC) do not rely on the collision resistance of the corresponding hash function, and therefore the recent attacks on SHA-1 have a significantly lower impact on the use of SHA-1 for HMAC. Because of this, the recommendation does not disable the hmac-sha1 MAC.

Solution

Note:

The commands below are written for the included DEFAULT system-wide crypto policy. If another policy is in use and follows local site policy, replace DEFAULT with the name of your system-wide crypto policy.

Multiple subpolicies may be assigned to a policy as a colon separated list. e.g. DEFAULT:NO-SHA1:NO-SSHCBC

The module for disabling SHA-1 is available from release 8.3 in /usr/share/crypto-policies/policies/modules/NO-SHA1.pmod. This may be copied to /etc/crypto-policies/policies/modules/NO-SHA1.pmod, verified, and used instead of creating a file ending in .pmod in the /etc/crypto-policies/policies/modules/ directory.

Any subpolicy not included in the update-crypto-policies --set command will not be applied to the system wide crypto policy.

Subpolicies must exist before they can be applied to the system wide crypto policy.

Create or edit a file in /etc/crypto-policies/policies/modules/ ending in .pmod and add or modify the following lines:

hash = -SHA1 sign = -*-SHA1 sha1_in_certs = 0

Example:

echo -e '# This is a subpolicy dropping the SHA1 hash and signature support hash = -SHA1 sign = -*-SHA1 sha1_in_certs = 0' > /etc/crypto-policies/policies/modules/NO-SHA1.pmod

Run the following command to update the system-wide cryptographic policy

update-crypto-policies --set <CRYPTO_POLICY>:<CRYPTO_SUBPOLICY1>:<CRYPTO_SUBPOLICY2>:<SUBPOLICY3>

Example:

update-crypto-policies --set DEFAULT:NO-SHA1

Run the following command to reboot the system to make your cryptographic settings effective for already running services and applications:

```
# reboot
```

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.13
800-171	3.5.2
800-171	3.13.8
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
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/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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - sha1_in_certs policy value
The command '/bin/grep -Pi -- '^\h*sha1_in_certs\h*=\h*' /etc/crypto-policies/state/CURRENT.pol'
 returned :

sha1_in_certs = 0

-------------------------
PASSED - Crypto policy settings for hash and sign
The command '/bin/grep -Pi -- '^\h*(hash|sign)\h*=\h*([^\r#]+)?-sha1\b' /etc/crypto-policies/state/
CURRENT.pol | /bin/awk -F: '{ print $NF } END {if (NR == 0) print "none"}'' returned :

none
```

1.6.3 Ensure system wide crypto policy disables cbc for ssh

Info

Cypher Block Chaining (CBC) is an algorithm that uses a block cipher.

Rationale:

A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext. If exploited, this attack can potentially allow an attacker to recover up to 32 bits of plaintext from an arbitrary block of ciphertext from a connection secured using the SSH protocol.

Impact:

CBC ciphers might be the only common cyphers when connecting to older SSH clients and servers

Solution

Note:

The commands below are written for the included DEFAULT system-wide crypto policy. If another policy is in use and follows local site policy, replace DEFAULT with the name of your system-wide crypto policy.

Multiple subpolicies may be assigned to a policy as a colon separated list. e.g. DEFAULT:NO-SHA1:NO-SSHCBC

Any subpolicy not included in the update-crypto-policies --set command will not be applied to the system wide crypto policy.

Subpolicies must exist before they can be applied to the system wide crypto policy.

Create or edit a file in /etc/crypto-policies/policies/modules/ ending in .pmod and add or modify one of the the following lines:

cipher@SSH = -*-CBC # Disables the CBC cipher for SSH

-OR-

cipher = -*-CBC # Disables the CBC cipher

Example:

echo -e '# This is a subpolicy to disable all CBC mode ciphers # for the SSH protocol (libssh and OpenSSH) cipher@SSH = -*-CBC' > /etc/crypto-policies/policies/modules/NO-SSHCBC.pmod

Run the following command to update the system-wide cryptographic policy

update-crypto-policies --set <CRYPTO_POLICY>:<CRYPTO_SUBPOLICY1>:<CRYPTO_SUBPOLICY2>:<SUBPOLICY3>

Example:

update-crypto-policies --set DEFAULT:NO-SHA1:NO-SSHCBC

Run the following command to reboot the system to make your cryptographic settings effective for already running services and applications:

```
# reboot
```

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.13
800-171	3.5.2
800-171	3.13.8
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
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/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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **

 - Cipher Block Chaining (CBC) is disabled for SSH
```

1.6.4 Ensure system wide crypto policy disables macs less than 128 bits

Info

Message Authentication Code (MAC) algorithm is a family of cryptographic functions that is parameterized by a symmetric key. Each of the functions can act on input data (called a 'message') of variable length to produce an output value of a specified length. The output value is called the MAC of the input message.

A MAC algorithm can be used to provide data-origin authentication and data-integrity protection

Rationale:

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 tunnel and capture credentials and information.

A MAC algorithm must be computationally infeasible to determine the MAC of a message without knowledge of the key, even if one has already seen the results of using that key to compute the MAC's of other messages.

Solution

Note:

The commands below are written for the included DEFAULT system-wide crypto policy. If another policy is in use and follows local site policy, replace DEFAULT with the name of your system-wide crypto policy.

Multiple subpolicies may be assigned to a policy as a colon separated list. e.g. DEFAULT:NO-SHA1:NO-SSHCBC:NO-WEAKMAC

Any subpolicy not included in the update-crypto-policies --set command will not be applied to the system wide crypto policy.

Subpolicies must exist before they can be applied to the system wide crypto policy.

Create or edit a file in /etc/crypto-policies/policies/modules/ ending in .pmod and add or modify one of the following lines:

mac = -*-64* # Disables weak macs

Example:

echo -e '# This is a subpolicy to disable weak macs mac = -*-64' > /etc/crypto-policies/policies/modules/NO-WEAKMAC.pmod

Run the following command to update the system-wide cryptographic policy

update-crypto-policies --set <CRYPTO_POLICY>:<CRYPTO_SUBPOLICY1>:<CRYPTO_SUBPOLICY2>:<SUBPOLICY3>

Example:

update-crypto-policies --set DEFAULT:NO-SHA1:NO-SSHCBC:NO-WEAKMAC

Run the following command to reboot the system to make your cryptographic settings effective for already running services and applications:

```
# reboot
```

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.13
800-171	3.5.2
800-171	3.13.8
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
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/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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: ^\h*mac\h*=\h*([^# \r]+)?-64\b file: /etc/crypto-policies/state/CURRENT.pol regex: ^\h*mac\h*=\h*([^# \r]+)?-64\b

Hosts

10.74.6.135

```
The file "/etc/crypto-policies/state/CURRENT.pol" does not contain "^\h*mac\h*=\h*([^#\n\r]+)?-64\b"
```

1.7.4 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.

Rationale:

-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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

file: /etc/motd group: root mask: 133 owner: root required: NO

Hosts

10.74.6.135

```
The file /etc/motd with fmode owner: root group: root mode: 0600 uid: 0 gid: 0 uneven permissions :
 FALSE is compliant with the policy value

/etc/motd
```

1.7.5 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.

Rationale:

-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)

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

file: /etc/issue group: root mask: 133 owner: root

Hosts

10.74.6.135

```
The file /etc/issue with fmode owner: root group: root mode: 0600 uid: 0 gid: 0 uneven permissions :
 FALSE is compliant with the policy value

/etc/issue
```

1.7.6 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.

Rationale:

-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)

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

file: /etc/issue.net group: root mask: 133 owner: root

Hosts

10.74.6.135

```
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
```

1.8.2 Ensure GDM login banner is configured

Info

GDM is the GNOME Display Manager which handles graphical login for GNOME based systems.

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place.

Solution

Run the following script to verify that the banner message is enabled and set:

#!/usr/bin/env bash

{ l_pkgoutput=''

if command -v dpkg-query > /dev/null 2>&1; then l_pq='dpkg-query -W'

elif command -v rpm > /dev/null 2>&1; then l_pq='rpm -q'

fi l_pcl='gdm gdm3' # Space seporated list of packages to check for l_pn in $l_pcl; do $l_pq '$l_pn' > /dev/null 2>&1 && l_pkgoutput='$l_pkgoutput

- Package: '$l_pn' exists on the system

- checking configuration'

done if [-n '$l_pkgoutput']; then

l_gdmprofile='gdm' # Set this to desired profile name IaW Local site policy l_bmessage=''Authorized uses only. All activity may be monitored and reported'' # Set to desired banner message if [! -f '/etc/dconf/profile/$l_gdmprofile']; then echo 'Creating profile '$l_gdmprofile''

echo -e 'user-db:user system-db:$l_gdmprofile file-db:/usr/share/$l_gdmprofile/greeter-dconf-defaults' > /etc/dconf/profile/$l_gdmprofile fi if [! -d '/etc/dconf/db/$l_gdmprofile.d/']; then echo 'Creating dconf database directory '/etc/dconf/db/$l_gdmprofile.d/''

mkdir /etc/dconf/db/$l_gdmprofile.d/ fi if ! grep -Piq '^h*banner-message-enableh*=h*trueb' /etc/dconf/db/$l_gdmprofile.d/*; then echo 'creating gdm keyfile for machine-wide settings'

if ! grep -Piq -- '^h*banner-message-enableh*=h*' /etc/dconf/db/$l_gdmprofile.d/*; then l_kfile='/etc/dconf/db/$l_gdmprofile.d/01-banner-message'

echo -e '

[org/gnome/login-screen] banner-message-enable=true' >> '$l_kfile'

else l_kfile='$(grep -Pil -- '^h*banner-message-enableh*=h*' /etc/dconf/db/$l_gdmprofile.d/*)'

! grep -Pq '^h*[org/gnome/login-screen]' '$l_kfile' && sed -ri '/^s*banner-message-enable/ i[org/gnome/login-screen]' '$l_kfile'

! grep -Pq '^h*banner-message-enableh*=h*trueb' '$l_kfile' && sed -ri 's/^s*(banner-message-enables*=s*)(S+)(s*.*$)/1true 3//' '$l_kfile'

sed -ri '/^s*[org/gnome/login-screen]/ a banner-message-enable=true' '$l_kfile'

fi fi if ! grep -Piq '^h*banner-message-text=['']+S+' '$l_kfile'; then sed -ri '/^s*banner-message-enable/abanner-message-text=$l_bmessage' '$l_kfile'

fi dconf update else echo -e '

- GNOME Desktop Manager isn't installed
- Recommendation is Not Applicable
- No remediation required '

fi }

Note:

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.

OR

Run the following command to remove the gdm package:

dnf remove gdm

Default Value:

disabled

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.9
800-53	AC-8
800-53R5	AC-8
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	AC-8
LEVEL	1A
NESA	M1.3.6
TBA-FIISB	45.2.4

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: PASS

Hosts

10.74.6.135

```
The command script with multiple lines returned :

- GNOME Desktop Manager isn't installed
 - Recommendation is Not Applicable
- Audit result:
  *** PASS ***


- Audit Result:
  ** PASS **
```

1.8.3 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

Rationale:

Displaying the user list eliminates half of the Userid/Password equation that an unauthorized person would need to log on.

Solution

Run the following script to enable the disable-user-list option:

Note: the l_gdm_profile variable in the script can be changed if a different profile name is desired in accordance with local site policy.

#!/usr/bin/env bash

{ l_gdmprofile='gdm'

if [! -f '/etc/dconf/profile/$l_gdmprofile']; then echo 'Creating profile '$l_gdmprofile''

echo -e 'user-db:user system-db:$l_gdmprofile file-db:/usr/share/$l_gdmprofile/greeter-dconf-defaults' > /etc/dconf/profile/$l_gdmprofile fi if [! -d '/etc/dconf/db/$l_gdmprofile.d/']; then echo 'Creating dconf database directory '/etc/dconf/db/$l_gdmprofile.d/''

mkdir /etc/dconf/db/$l_gdmprofile.d/ fi if ! grep -Piq '^h*disable-user-listh*=h*trueb' /etc/dconf/db/$l_gdmprofile.d/*; then echo 'creating gdm keyfile for machine-wide settings'

if ! grep -Piq -- '^h*[org/gnome/login-screen]' /etc/dconf/db/$l_gdmprofile.d/*; then echo -e '

[org/gnome/login-screen] # Do not show the user list disable-user-list=true' >> /etc/dconf/db/$l_gdmprofile.d/00-login-screen else sed -ri '/^s*[org/gnome/login-screen]/ a# Do not show the user list disable-user-list=true' $(grep -Pil -- '^h*[org/gnome/login-screen]' /etc/dconf/db/$l_gdmprofile.d/*) fi fi 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.

OR Run the following command to remove the GNOME package:

dnf remove gdm

Default Value:

false

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.6
800-171	3.4.7
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
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

- GNOME Desktop Manager isn't installed
 - Recommendation is Not Applicable
- Audit result:
  *** PASS ***
```

1.8.4 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.

idle-delay=uint32 {n} - Number of seconds of inactivity before the screen goes blank

lock-delay=uint32 {n} - Number of seconds after the screen is blank before locking the screen

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 900

Specify the dconf path

[org/gnome/desktop/screensaver]

Number of seconds after the screen is blank before locking the screen

lock-delay=uint32 5

Rationale:

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

Create or edit a file 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.

Example:

echo -e '

user-db:user system-db:local' >> /etc/dconf/profile/user

Create the directory /etc/dconf/db/{NAME_OF_DCONF_DATABASE}.d/ if it doesn't already exist:

Example:

mkdir /etc/dconf/db/local.d

Create the key file '/etc/dconf/db/{NAME_OF_DCONF_DATABASE}.d/{FILE_NAME} to provide information for the {NAME_OF_DCONF_DATABASE} database:

Example script:

#!/usr/bin/env bash

{ l_key_file='/etc/dconf/db/local.d/00-screensaver'

l_idmv='900' # Set max value for idle-delay in seconds (between 1 and 900) l_ldmv='5' # Set max value for lock-delay in seconds (between 0 and 5) { echo '# Specify the dconf path'

echo '[org/gnome/desktop/session]'

echo ''

echo '# Number of seconds of inactivity before the screen goes blank'

echo '# Set to 0 seconds if you want to deactivate the screensaver.'

echo 'idle-delay=uint32 $l_idmv'

echo ''

echo '# Specify the dconf path'

echo '[org/gnome/desktop/screensaver]'

echo ''

echo '# Number of seconds after the screen is blank before locking the screen'

echo 'lock-delay=uint32 $l_ldmv'

} > '$l_key_file'

}

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

Run the following command to update the system databases:

dconf update

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

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.1
800-171	3.1.10
800-171	3.1.11
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(a)(2)(iii)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **

 - GNOME Desktop Manager package is not installed on the system
  - Recommendation is not applicable
```

1.8.5 Ensure GDM screen locks cannot be overridden

Info

GNOME Desktop Manager can make the screen lock automatically whenever the user is idle for some amount of time.

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.

Example Lock File:

Lock desktop screensaver settings

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

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

Rationale:

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

Run the following script to ensure screen locks cannot be overridden:

#!/usr/bin/env bash

{ # Check if GNMOE Desktop Manager is installed. If package isn't installed, recommendation is Not Applicable

determine system's package manager l_pkgoutput=''

if command -v dpkg-query > /dev/null 2>&1; then l_pq='dpkg-query -W'

elif command -v rpm > /dev/null 2>&1; then l_pq='rpm -q'

fi # Check if GDM is installed l_pcl='gdm gdm3' # Space seporated list of packages to check for l_pn in $l_pcl; do $l_pq '$l_pn' > /dev/null 2>&1 && l_pkgoutput='y' && echo -e '

- Package: '$l_pn' exists on the system

- remediating configuration if needed'

done # Check configuration (If applicable) if [-n '$l_pkgoutput']; then # Look for idle-delay to determine profile in use, needed for remaining tests l_kfd='/etc/dconf/db/$(grep -Psril '^h*idle-delayh*=h*uint32h +d+b' /etc/dconf/db/*/ | awk -F'/' '{split($(NF-1),a,'.');print a[1]}').d' #set directory of key file to be locked # Look for lock-delay to determine profile in use, needed for remaining tests l_kfd2='/etc/dconf/db/$(grep -Psril '^h*lock-delayh*=h*uint32h+d+b' /etc/dconf/db/*/ | awk -F'/' '{split($(NF-1),a,'.');print a[1]}').d' #set directory of key file to be locked if [-d '$l_kfd']; then # If key file directory doesn't exist, options can't be locked if grep -Prilq '^h*/org/gnome/desktop/session/idle-delayb' '$l_kfd'; then echo ' - 'idle-delay' is locked in '$(grep -Pril '^h*/org/gnome/desktop/session/idle-delayb' '$l_kfd')''

else echo 'creating entry to lock 'idle-delay''

[! -d '$l_kfd'/locks] && echo 'creating directory $l_kfd/locks' && mkdir '$l_kfd'/locks { echo -e '

Lock desktop screensaver idle-delay setting'

echo '/org/gnome/desktop/session/idle-delay'

} >> '$l_kfd'/locks/00-screensaver fi else echo -e ' - 'idle-delay' is not set so it can not be locked

- Please follow Recommendation 'Ensure GDM screen locks when the user is idle' and follow this Recommendation again'

fi if [-d '$l_kfd2']; then # If key file directory doesn't exist, options can't be locked if grep -Prilq '^h*/org/gnome/desktop/screensaver/lock-delayb' '$l_kfd2'; then echo ' - 'lock-delay' is locked in '$(grep -Pril '^h*/org/gnome/desktop/screensaver/lock-delayb' '$l_kfd2')''

else echo 'creating entry to lock 'lock-delay''

[! -d '$l_kfd2'/locks] && echo 'creating directory $l_kfd2/locks' && mkdir '$l_kfd2'/locks { echo -e '

Lock desktop screensaver lock-delay setting'

echo '/org/gnome/desktop/screensaver/lock-delay'

} >> '$l_kfd2'/locks/00-screensaver fi else echo -e ' - 'lock-delay' is not set so it can not be locked

- Please follow Recommendation 'Ensure GDM screen locks when the user is idle' and follow this Recommendation again'

fi else echo -e ' - GNOME Desktop Manager package is not installed on the system

- Recommendation is not applicable'

fi }

Run the following command to update the system databases:

dconf update

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

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.1
800-171	3.1.10
800-171	3.1.11
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(a)(2)(iii)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **

 - GNOME Desktop Manager package is not installed on the system
  - Recommendation is not applicable
```

1.8.6 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.

Rationale:

With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.

Impact:

The use of portable hard drives is very common for workstation users. If your organization allows the use of portable storage or media on workstations and physical access controls to workstations is considered adequate there is little value add in turning off automounting.

Solution

Run the following script to disable automatic mounting of media for all GNOME users:

#!/usr/bin/env bash

{ l_pkgoutput=''

l_gpname='local' # Set to desired dconf profile name (default is local) # Check if GNOME Desktop Manager is installed. If package isn't installed, recommendation is Not Applicable

determine system's package manager if command -v dpkg-query > /dev/null 2>&1; then l_pq='dpkg-query -W'

elif command -v rpm > /dev/null 2>&1; then l_pq='rpm -q'

fi # Check if GDM is installed l_pcl='gdm gdm3' # Space seporated list of packages to check for l_pn in $l_pcl; do $l_pq '$l_pn' > /dev/null 2>&1 && l_pkgoutput='$l_pkgoutput

- Package: '$l_pn' exists on the system

- checking configuration'

done # Check configuration (If applicable) if [-n '$l_pkgoutput']; then echo -e '$l_pkgoutput'

Look for existing settings and set variables if they exist l_kfile='$(grep -Prils -- '^h*automountb' /etc/dconf/db/*.d)'

l_kfile2='$(grep -Prils -- '^h*automount-openb' /etc/dconf/db/*.d)'

Set profile name based on dconf db directory ({PROFILE_NAME}.d) if [-f '$l_kfile']; then l_gpname='$(awk -F/ '{split($(NF-1),a,'.');print a[1]}' <<< '$l_kfile')'

echo ' - updating dconf profile name to '$l_gpname''

elif [-f '$l_kfile2']; then l_gpname='$(awk -F/ '{split($(NF-1),a,'.');print a[1]}' <<< '$l_kfile2')'

echo ' - updating dconf profile name to '$l_gpname''

fi # check for consistency (Clean up configuration if needed) if [-f '$l_kfile'] && ['$(awk -F/ '{split($(NF-1),a,'.');print a[1]}' <<< '$l_kfile')' != '$l_gpname']; then sed -ri '/^s*automounts*=/s/^/# /' '$l_kfile'

l_kfile='/etc/dconf/db/$l_gpname.d/00-media-automount'

fi if [-f '$l_kfile2'] && ['$(awk -F/ '{split($(NF-1),a,'.');print a[1]}' <<< '$l_kfile2')' != '$l_gpname']; then sed -ri '/^s*automount-opens*=/s/^/# /' '$l_kfile2'

fi [-z '$l_kfile'] && l_kfile='/etc/dconf/db/$l_gpname.d/00-media-automount'

Check if profile file exists if grep -Pq -- '^h*system-db:$l_gpnameb' /etc/dconf/profile/*; then echo -e '

- dconf database profile exists in: '$(grep -Pl -- '^h*system-db:$l_gpnameb' /etc/dconf/profile/*)''

else if [! -f '/etc/dconf/profile/user']; then l_gpfile='/etc/dconf/profile/user'

else l_gpfile='/etc/dconf/profile/user2'

fi echo -e ' - creating dconf database profile'

{ echo -e '

user-db:user'

echo 'system-db:$l_gpname'

} >> '$l_gpfile'

fi # create dconf directory if it doesn't exists l_gpdir='/etc/dconf/db/$l_gpname.d'

if [-d '$l_gpdir']; then echo ' - The dconf database directory '$l_gpdir' exists'

else echo ' - creating dconf database directory '$l_gpdir''

mkdir '$l_gpdir'

fi # check automount-open setting if grep -Pqs -- '^h*automount-openh*=h*falseb' '$l_kfile'; then echo ' - 'automount-open' is set to false in: '$l_kfile''

else echo ' - creating 'automount-open' entry in '$l_kfile''

! grep -Psq -- '^h*[org/gnome/desktop/media-handling]b' '$l_kfile' && echo '[org/gnome/desktop/media-handling]' >> '$l_kfile'

sed -ri '/^s*[org/gnome/desktop/media-handling]/a automount-open=false' '$l_kfile'

fi # check automount setting if grep -Pqs -- '^h*automounth*=h*falseb' '$l_kfile'; then echo ' - 'automount' is set to false in: '$l_kfile''

else echo ' - creating 'automount' entry in '$l_kfile''

! grep -Psq -- '^h*[org/gnome/desktop/media-handling]b' '$l_kfile' && echo '[org/gnome/desktop/media-handling]' >> '$l_kfile'

sed -ri '/^s*[org/gnome/desktop/media-handling]/a automount=false' '$l_kfile'

fi # update dconf database dconf update else echo -e '

- GNOME Desktop Manager package is not installed on the system

- Recommendation is not applicable'

fi }

OR Run the following command to uninstall the GNOME desktop Manager package:

dnf remove gdm

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.8.7
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/IEC-27001	A.8.3.1
ISO/IEC-27001	A.8.3.3
LEVEL	1A
LEVEL	2A
NESA	T1.4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **

 - GNOME Desktop Manager package is not installed on the system
  - Recommendation is not applicable
```

1.8.7 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.

Example Lock File:

Lock automount settings

/org/gnome/desktop/media-handling/automount

/org/gnome/desktop/media-handling/automount-open

Rationale:

With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.

Impact:

The use of portable hard drives is very common for workstation users

Solution

Run the following script to lock disable automatic mounting of media for all GNOME users:

#!/usr/bin/env bash

{ # Check if GNMOE Desktop Manager is installed. If package isn't installed, recommendation is Not Applicable

determine system's package manager l_pkgoutput=''

if command -v dpkg-query > /dev/null 2>&1; then l_pq='dpkg-query -W'

elif command -v rpm > /dev/null 2>&1; then l_pq='rpm -q'

fi # Check if GDM is installed l_pcl='gdm gdm3' # Space seporated list of packages to check for l_pn in $l_pcl; do $l_pq '$l_pn' > /dev/null 2>&1 && l_pkgoutput='y' && echo -e '

- Package: '$l_pn' exists on the system

- remediating configuration if needed'

done # Check configuration (If applicable) if [-n '$l_pkgoutput']; then # Look for automount to determine profile in use, needed for remaining tests l_kfd='/etc/dconf/db/$(grep -Psril '^h*automountb' /etc/dconf/db/*/ | awk -F'/' '{split($(NF-1),a,'.');print a[1]}').d' #set directory of key file to be locked # Look for automount-open to determine profile in use, needed for remaining tests l_kfd2='/etc/dconf/db/$(grep -Psril '^h*automount-openb' /etc/dconf/db/*/ | awk -F'/' '{split($(NF-1),a,'.');print a[1]}').d' #set directory of key file to be locked if [-d '$l_kfd']; then # If key file directory doesn't exist, options can't be locked if grep -

Priq '^h*/org/gnome/desktop/media-handling/automountb' '$l_kfd'; then echo ' - 'automount' is locked in '$(grep -Pril '^h*/org/gnome/desktop/media-handling/automountb' '$l_kfd')''

else echo ' - creating entry to lock 'automount''

[! -d '$l_kfd'/locks] && echo 'creating directory $l_kfd/locks' && mkdir '$l_kfd'/locks { echo -e '

Lock desktop media-handling automount setting'

echo '/org/gnome/desktop/media-handling/automount'

} >> '$l_kfd'/locks/00-media-automount fi else echo -e ' - 'automount' is not set so it can not be locked

- Please follow Recommendation 'Ensure GDM automatic mounting of removable media is disabled' and follow this Recommendation again'

fi if [-d '$l_kfd2']; then # If key file directory doesn't exist, options can't be locked if grep -Priq '^h*/org/gnome/desktop/media-handling/automount-openb' '$l_kfd2'; then echo ' - 'automount-open' is locked in '$(grep -Pril '^h*/org/gnome/desktop/media-handling/automount-openb' '$l_kfd2')''

else echo ' - creating entry to lock 'automount-open''

[! -d '$l_kfd2'/locks] && echo 'creating directory $l_kfd2/locks' && mkdir '$l_kfd2'/locks { echo -e '

Lock desktop media-handling automount-open setting'

echo '/org/gnome/desktop/media-handling/automount-open'

} >> '$l_kfd2'/locks/00-media-automount fi else echo -e ' - 'automount-open' is not set so it can not be locked

- Please follow Recommendation 'Ensure GDM automatic mounting of removable media is disabled' and follow this Recommendation again'

fi # update dconf database dconf update else echo -e ' - GNOME Desktop Manager package is not installed on the system

- Recommendation is not applicable'

fi }

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.8.7
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/IEC-27001	A.8.3.1
ISO/IEC-27001	A.8.3.3
LEVEL	1A

LEVEL	2A
NESA	T1.4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **

 - GNOME Desktop Manager package is not installed on the system
  - Recommendation is not applicable
```

1.8.8 Ensure GDM autorun-never is enabled

Info

The autorun-never setting allows the GNOME Desktop Display Manager to disable autorun through GDM.

Rationale:

Malware on removable media may take advantage of Autorun features when the media is inserted into a system and execute.

Solution

Run the following script to set autorun-never to true for GDM users:

#!/usr/bin/env bash

{ l_pkgoutput='' l_output='' l_output2=''

l_gpname='local' # Set to desired dconf profile name (default is local) # Check if GNOME Desktop Manager is installed. If package isn't installed, recommendation is Not Applicable

determine system's package manager if command -v dpkg-query > /dev/null 2>&1; then l_pq='dpkg-query -W'

elif command -v rpm > /dev/null 2>&1; then l_pq='rpm -q'

fi # Check if GDM is installed l_pcl='gdm gdm3' # Space separated list of packages to check for l_pn in $l_pcl; do $l_pq '$l_pn' > /dev/null 2>&1 && l_pkgoutput='$l_pkgoutput

- Package: '$l_pn' exists on the system

- checking configuration'

done echo -e '$l_pkgoutput'

Check configuration (If applicable) if [-n '$l_pkgoutput']; then echo -e '$l_pkgoutput'

Look for existing settings and set variables if they exist l_kfile='$(grep -Prils -- '^h*autorun-neverb' /etc/dconf/db/*.d)'

Set profile name based on dconf db directory ({PROFILE_NAME}.d) if [-f '$l_kfile']; then l_gpname='$(awk -F/ '{split($(NF-1),a,'.');print a[1]}' <<< '$l_kfile')'

echo ' - updating dconf profile name to '$l_gpname''

fi [! -f '$l_kfile'] && l_kfile='/etc/dconf/db/$l_gpname.d/00-media-autorun'

Check if profile file exists if grep -Pq -- '^h*system-db:$l_gpnameb' /etc/dconf/profile/*; then echo -e '

- dconf database profile exists in: '$(grep -Pl -- '^h*system-db:$l_gpnameb' /etc/dconf/profile/*)''

else [! -f '/etc/dconf/profile/user'] && l_gpfile='/etc/dconf/profile/user' || l_gpfile='/etc/dconf/profile/user2'

echo -e ' - creating dconf database profile'

{ echo -e '

user-db:user'

echo 'system-db:$l_gpname'

} >> '$l_gpfile'

fi # create dconf directory if it doesn't exists l_gpdir='/etc/dconf/db/$l_gpname.d'

if [-d '$l_gpdir']; then echo ' - The dconf database directory '$l_gpdir' exists'

else echo ' - creating dconf database directory '$l_gpdir''

mkdir '$l_gpdir'

fi # check autorun-never setting if grep -Pqs -- '^h*autorun-neverh*=h*trueb' '$l_kfile'; then echo ' - 'autorun-never' is set to true in: '$l_kfile''

else echo ' - creating or updating 'autorun-never' entry in '$l_kfile''

if grep -Psq -- '^h*autorun-never' '$l_kfile'; then sed -ri 's/(^s*autorun-nevers*=s*)(S+)(s*.*)$/1true 3/' '$l_kfile'

else ! grep -Psq -- '^h*[org/gnome/desktop/media-handling]b' '$l_kfile' && echo '[org/gnome/desktop/media-handling]' >> '$l_kfile'

sed -ri '/^s*[org/gnome/desktop/media-handling]/a autorun-never=true' '$l_kfile'

fi fi else echo -e '

- GNOME Desktop Manager package is not installed on the system

- Recommendation is not applicable'

fi # update dconf database dconf update }

Default Value:

false

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.8.7
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/IEC-27001	A.8.3.1
ISO/IEC-27001	A.8.3.3
LEVEL	1A
NESA	T1.4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **

 - GNOME Desktop Manager package is not installed on the system
  - Recommendation is not applicable
```

1.8.9 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.

Example Lock File:

Lock desktop media-handling settings

/org/gnome/desktop/media-handling/autorun-never

Rationale:

Malware on removable media may take advantage of Autorun features when the media is inserted into a system and execute.

Solution

Run the following script to ensure that autorun-never=true cannot be overridden:

#!/usr/bin/env bash

{ # Check if GNOME Desktop Manager is installed. If package isn't installed, recommendation is Not Applicable

determine system's package manager l_pkgoutput=''

if command -v dpkg-query > /dev/null 2>&1; then l_pq='dpkg-query -W'

elif command -v rpm > /dev/null 2>&1; then l_pq='rpm -q'

fi # Check if GDM is installed l_pcl='gdm gdm3' # Space separated list of packages to check for l_pn in $l_pcl; do $l_pq '$l_pn' > /dev/null 2>&1 && l_pkgoutput='y' && echo -e '

- Package: '$l_pn' exists on the system

- remediating configuration if needed'

done # Check configuration (If applicable) if [-n '$l_pkgoutput']; then # Look for autorun to determine profile in use, needed for remaining tests l_kfd='/etc/dconf/db/$(grep -Psril '^h*autorun-neverb' /etc/dconf/db/*/ | awk -F'/' '{split($(NF-1),a,'.');print a[1]}').d' #set directory of key file to be locked if [-d '$l_kfd']; then # If key file directory doesn't exist, options can't be locked if grep -Priq '^h*/org/gnome/desktop/media-handling/autorun-neverb' '$l_kfd'; then echo ' - 'autorun-never' is locked in '$(grep -Pril '^h*/org/gnome/desktop/media-handling/autorun-neverb' '$l_kfd')''

else echo ' - creating entry to lock 'autorun-never''

[! -d '$l_kfd'/locks] && echo 'creating directory $l_kfd/locks' && mkdir '$l_kfd'/locks { echo -e '

Lock desktop media-handling autorun-never setting'

echo '/org/gnome/desktop/media-handling/autorun-never'

} >> '$l_kfd'/locks/00-media-autorun fi else echo -e ' - 'autorun-never' is not set so it can not be locked

- Please follow Recommendation 'Ensure GDM autorun-never is enabled' and follow this Recommendation again'

fi # update dconf database dconf update else echo -e ' - GNOME Desktop Manager package is not installed on the system

- Recommendation is not applicable'

fi }

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.8.7
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/IEC-27001	A.8.3.1
ISO/IEC-27001	A.8.3.3
LEVEL	1A
NESA	T1.4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **

 - GNOME Desktop Manager package is not installed on the system
  - Recommendation is not applicable
```

1.8.10 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

Rationale:

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 the file /etc/gdm/custom.conf and remove the line:

Enable=true

Default Value:

false (This is denoted by no Enabled= entry in the file /etc/gdm/custom.conf in the [xdmcp] section

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A

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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

2.1.1 Ensure time synchronization 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: If another method for time synchronization is being used, this section may be skipped.

Rationale:

Time synchronization is important to support time sensitive security mechanisms like Kerberos and also ensures log files have consistent time records across the enterprise, which aids in forensic investigations.

Solution

Run the following command to install chrony:

dnf install chrony

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.6
800-171	3.3.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: gt required: YES rpm: chrony-0.0.0-0

Hosts

10.74.6.135

```
The local RPM is newer than chrony-0.0.0-0 (chrony-4.2-1.0.1.el8)
```

2.1.3 Ensure chrony is not run as the root user

Info

The file /etc/sysconfig/chronyd allows configuration of options for chrony to include the user chrony is run as. By default this is set to the user chrony

Rationale:

Services should not be set to run as the root user

Solution

Edit the file /etc/sysconfig/chronyd and add or modify the following line:

OPTIONS='-u chrony'

Run the following command to reload the chronyd.service configuration:

systemctl try-reload-or-restart chronyd.service

Default Value:

OPTIONS='-u chrony'

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.5
800-53	AC-6
800-53R5	AC-6
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
CSF	PR.DS-5
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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
QCSC-V1	13.2
SWIFT-CSCV1	5.1
TBA-FIISB	31.4.2
TBA-FIISB	31.4.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: /bin/grep -Psi -- '^\h*OPTIONS=\"?.*-u\h+root\b' /etc/sysconfig/chronyd | /bin/awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}'

expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command '/bin/grep -Psi -- '^\h*OPTIONS=\"?.*-u\h+root\b' /etc/sysconfig/chronyd | /bin/awk
 '{print} END {if (NR == 0) print "pass" ; else print "fail"}'' returned :

pass
```

2.2.1 Ensure autofs services are not in use

Info

autofs allows automatic mounting of devices, typically including CD/DVDs and USB drives.

Rationale:

With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.

Impact:

The use of portable hard drives is very common for workstation users. If your organization allows the use of portable storage or media on workstations and physical access controls to workstations is considered adequate there is little value add in turning off automounting.

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.

Solution

Run the following commands to stop autofs.service and remove autofs package:

systemctl stop autofs.service # dnf remove 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

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.8.7
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/IEC-27001	A.8.3.1
ISO/IEC-27001	A.8.3.3
LEVEL	1A
LEVEL	2A
NESA	T1.4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - autofs.service active
The command '/bin/systemctl is-active autofs.service 2>/dev/null | /bin/grep '^active' | /bin/awk
 '{print} END {if (NR == 0) print "pass" ; else print "fail"}'' returned :

pass

-------------------------
PASSED - autofs.service enabled
The command '/bin/systemctl is-enabled autofs.service 2>/dev/null | /bin/grep 'enabled' | /bin/awk
 '{print} END {if (NR == 0) print "pass" ; else print "fail"}'' returned :

pass
```

2.2.2 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.

Rationale:

Automatic discovery of network services is not normally required for system functionality. It is recommended to remove this package to reduce the potential attack surface.

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.

Solution

Run the following commands to stop avahi-daemon.socket and avahi-daemon.service, and remove the avahi package:

systemctl stop avahi-daemon.socket avahi-daemon.service # dnf remove avahi

-OR-

-IF- the avahi 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

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
LEVEL	2A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lte rpm: avahi-0.0.0-0

Hosts

10.74.6.135

```
The package 'avahi-0.0.0-0' is not installed
```

2.2.3 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.

Rationale:

Unless a system is specifically set up to act as a DHCP server, it is recommended that the dhcp-server package be removed to reduce the potential attack surface.

Impact:

There may be packages that are dependent on the dhcp-server package. If the dhcp-server package is removed, these dependent packages will be removed as well. Before removing the 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 dhcpd.service and dhcpd6.service leaving the dhcp-server package installed.

Solution

Run the following commands to stop dhcpd.service and dhcpd6.service and remove dhcp-server package:

systemctl stop dhcpd.service dhcpd6.service # dnf remove dhcp-server

-OR-

-IF- the dhcp-server package is required as a dependency:

Run the following commands to stop and mask dhcpd.service and dhcpd6.service:

systemctl stop dhcpd.service dhcpd6.service # systemctl mask dhcpd.service dhcpd6.service

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lte rpm: dhcp-server-0.0.0-0

Hosts

10.74.6.135

```
The package 'dhcp-server-0.0.0-0' is not installed
```

2.2.4 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.

Rationale:

Unless a system is specifically designated to act as a DNS server, it is recommended that the package be removed to reduce the potential attack surface.

Impact:

There may be packages that are dependent on the bind package. If the bind package is removed, these dependent packages will be removed as well. Before removing the bind package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask the named.service leaving the bind package installed.

Solution

Run the following commands to stop named.service and remove bind package:

systemctl stop named.service # dnf remove bind

-OR-

-IF- the bind package is required as a dependency:

Run the following commands to stop and mask named.service:

systemctl stop named.service # systemctl mask named.service

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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

GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lte rpm: bind-0.0.0-0

Hosts

10.74.6.135

```
The package 'bind-0.0.0-0' is not installed
```

2.2.5 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.

Rationale:

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.

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.

Solution

Run the following commands to stop dnsmasq.service and remove dnsmasq package:

systemctl stop dnsmasq.service # dnf remove 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

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lte rpm: dnsmasq-0.0.0-0

Hosts

10.74.6.135

```
The package 'dnsmasq-0.0.0-0' is not installed
```

2.2.6 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.

Rationale:

If there is no need to mount directories and file systems to Windows systems, then this package can be removed to reduce the potential attack surface.

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 smb.service leaving the samba package installed.

Solution

Run the following command to stop smb.service and remove samba package:

systemctl stop smb.service # dnf remove samba

-OR-

-IF- the samba package is required as a dependency:

Run the following commands to stop and mask the smb.service:

systemctl stop smb.service # systemctl mask smb.service

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lte rpm: samba-0.0.0-0

Hosts

10.74.6.135

```
The package 'samba-0.0.0-0' is not installed
```

2.2.7 Ensure ftp server services are not in use

Info

FTP (File Transfer Protocol) is a traditional and widely used standard tool for transferring files between a server and clients over a network, especially where no authentication is necessary (permits anonymous users to connect to a server).

Rationale:

Unless there is a need to run the system as a FTP server, it is recommended that the package be removed to reduce the potential attack surface.

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.

Solution

Run the following commands to stop vsftpd.service and remove vsftpd package:

systemctl stop vsftpd.service # dnf remove 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.

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lte rpm: vsftpd-0.0.0-0

Hosts

10.74.6.135

```
The package 'vsftpd-0.0.0-0' is not installed
```

2.2.8 Ensure message access server services are not in use

Info

dovecot and cyrus-imapd are open source IMAP and POP3 server packages for Linux based systems.

Rationale:

Unless POP3 and/or IMAP servers are to be provided by this system, it is recommended that the package be removed to reduce the potential attack surface.

Note: Several IMAP/POP3 servers exist and can use other service names. These should also be audited and the packages removed if not required.

Impact:

There may be packages that are dependent on dovecot and cyrus-imapd packages. If dovecot and cyrus-imapd packages are removed, these dependent packages will be removed as well. Before removing dovecot and cyrus-imapd 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, dovecot.service and cyrus-imapd.service leaving dovecot and cyrus-imapd packages installed.

Solution

Run the following commands to stop dovecot.socket, dovecot.service, and cyrus-imapd.service, and remove dovecot and cyrus-imapd packages:

systemctl stop dovecot.socket dovecot.service cyrus-imapd.service # dnf remove dovecot cyrus-imapd

-OR-

-IF- a package is installed and is required for dependencies:

Run the following commands to stop and mask dovecot.socket, dovecot.service, and cyrus-imapd.service:

systemctl stop dovecot.socket dovecot.service cyrus-imapd.service # systemctl mask dovecot.socket dovecot.service cyrus-imapd.service

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - cyrus-imapd exist on the system
The package 'cyrus-imapd-0.0.0-0' is not installed

-------------------------
PASSED - dovecot exist on the system
The package 'dovecot-0.0.0-0' is not installed
```

2.2.9 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.

Rationale:

If the system does not require access to network shares or the ability to provide network file system services for other host's network shares, it is recommended that the nfs-utils package be removed to reduce the attack surface of the system.

Impact:

Many of the libvirt packages used by Enterprise Linux virtualization are dependent on the nfs-utils package. If the nfs-utils package is removed, these dependent packages will be removed as well. Before removing the nfs-utils 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-utils package installed.

Solution

Run the following command to stop nfs-server.service and remove nfs-utils package:

systemctl stop nfs-server.service # dnf remove nfs-utils

-OR-

-IF- the nfs-utils 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

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - nfs-server.service enabled
The command '/bin/systemctl is-enabled nfs-server.service 2>/dev/null | /bin/grep 'enabled' | /bin/
awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}'' returned :

pass

-------------------------
PASSED - nfs-server.service active
The command '/bin/systemctl is-active nfs-server.service 2>/dev/null | /bin/grep '^active' | /bin/
awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}'' returned :

pass
```

2.2.10 Ensure nis server services are not in use

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 (ypbind) was used to bind a machine to an NIS server and receive the distributed configuration files.

Rationale:

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed.

Impact:

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.

Solution

Run the following commands to stop ypserv.service and remove ypserv package:

systemctl stop ypserv.service # dnf remove 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

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lte rpm: ypserv-0.0.0-0

Hosts

10.74.6.135

```
The package 'ypserv-0.0.0-0' is not installed
```

2.2.11 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.

Rationale:

If the system does not need to print jobs or accept print jobs from other systems, it is recommended that CUPS be removed to reduce the potential attack surface.

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.

Solution

Run the following commands to stop cups.socket and cups.service, and remove the cups package:

systemctl stop cups.socket cups.service # dnf remove 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

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lte rpm: cups-0.0.0-0

Hosts

10.74.6.135

```
The package 'cups-0.0.0-0' is not installed
```

2.2.12 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.

Rationale:

A small request (~82 bytes via UDP) sent to the Portmapper generates a large response (7x to 28x amplification), which makes it a suitable tool for DDoS attacks. If rpcbind is not required, it is recommended to remove rpcbind package to reduce the potential attack surface.

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.

Solution

Run the following commands to stop rpcbind.socket and rpcbind.service, and remove the rpcbind package:

systemctl stop rpcbind.socket rpcbind.service # dnf remove 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

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7

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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - rpcbind.socket rpcbind.service active
The command '/bin/systemctl is-active rpcbind.socket rpcbind.service 2>/dev/null | /bin/grep
 '^active' | /bin/awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}'' returned :

pass

-------------------------
PASSED - rpcbind.socket rpcbind.service enabled
The command '/bin/systemctl is-enabled rpcbind.socket rpcbind.service 2>/dev/null | /bin/grep
 'enabled' | /bin/awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}'' returned :

pass
```

2.2.13 Ensure rsync services are not in use

Info

The rsyncd.service can be used to synchronize files between systems over network links.

Rationale:

Unless required, the rsync-daemon package should be removed to reduce the potential attack surface.

The rsyncd.service presents a security risk as it uses unencrypted protocols for communication.

Impact:

There may be packages that are dependent on the rsync-daemon package. If the rsync-daemon package is removed, these dependent packages will be removed as well. Before removing the rsync-daemon package, review any dependent packages to determine if they are required on the system.

-IF- a dependent package is required: stop and mask the rsyncd.socket and rsyncd.service leaving the rsync-daemon package installed.

Solution

Run the following commands to stop rsyncd.socket and rsyncd.service, and remove the rsync-daemon package:

systemctl stop rsyncd.socket rsyncd.service # dnf remove rsync-daemon

-OR-

-IF- the rsync-daemon package is required as a dependency:

Run the following commands to stop and mask the rsyncd.socket and rsyncd.service:

systemctl stop rsyncd.socket rsyncd.service # systemctl mask rsyncd.socket rsyncd.service

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lte rpm: rsync-daemon-0.0.0-0

Hosts

10.74.6.135

```
The package 'rsync-daemon-0.0.0-0' is not installed
```

2.2.14 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.

Rationale:

The SNMP server can communicate using SNMPv1, which transmits data in the clear and does not require authentication to execute commands. SNMPv3 replaces the simple/clear text password sharing used in SNMPv2 with more securely encoded parameters. If the the SNMP service is not required, the net-snmp package should be removed to reduce the attack surface of the system.

Note: If SNMP is required:

The server should be configured for SNMP v3 only. User Authentication and Message Encryption should be configured.

If SNMP v2 is absolutely necessary, modify the community strings' values.

Impact:

There may be packages that are dependent on the net-snmp package. If the net-snmp package is removed, these packages will be removed as well.

Before removing the net-snmp 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 net-snmp package installed.

Solution

Run the following commands to stop snmpd.service and remove net-snmp package:

systemctl stop snmpd.service # dnf remove net-snmp

-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

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lte rpm: net-snmp-0.0.0-0

Hosts

10.74.6.135

```
The package 'net-snmp-0.0.0-0' is not installed
```

2.2.15 Ensure telnet server services are not in use

Info

The telnet-server package contains the telnet daemon, which accepts connections from users from other systems via the telnet protocol.

Rationale:

The telnet protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow a user with access to sniff network traffic the ability to steal credentials. The ssh package provides an encrypted session and stronger security.

Impact:

There may be packages that are dependent on the telnet-server package. If the telnet-server package is removed, these dependent packages will be removed as well. Before removing the telnet-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 telnet.socket leaving the telnet-server package installed.

Solution

Run the following commands to stop telnet.socket and remove the telnet-server package:

systemctl stop telnet.socket # dnf remove telnet-server

-OR-

-IF- a package is installed and is required for dependencies:

Run the following commands to stop and mask telnet.socket:

systemctl stop telnet.socket # systemctl mask telnet.socket

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-53	CM-6
800-53	CM-7
800-53R5	CM-6
800-53R5	CM-7
CSCV7	2.6
CSCV7	9.2
CSCV8	4.8

CSF	PR.IP-1
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lte rpm: telnet-server-0.0.0-0

Hosts

10.74.6.135

```
The package 'telnet-server-0.0.0-0' is not installed
```

2.2.16 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.

Rationale:

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

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 tftp-server package. If the tftp-server package is removed, these dependent packages will be removed as well. Before removing the tftp-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 tftp.socket and tftp.service leaving the tftp-server package installed.

Solution

Run the following commands to stop tftp.socket and tftp.service, and remove the tftp-server package:

systemctl stop tftp.socket tftp.service # dnf remove tftp-server

-OR-

-IF- the tftp-server package is required as a dependency:

Run the following commands to stop and mask tftp.socket and tftp.service:

systemctl stop tftp.socket tftp.service # systemctl mask tftp.socket tftp.service

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lte rpm: tftp-server-0.0.0-0

Hosts

10.74.6.135

```
The package 'tftp-server-0.0.0-0' is not installed
```

2.2.17 Ensure web proxy server services are not in use

Info

Squid is a standard proxy server used in many distributions and environments.

Rationale:

Unless a system is specifically set up to act as a proxy server, it is recommended that the squid package be removed to reduce the potential attack surface.

Note: Several HTTP proxy servers exist. These should be checked and removed unless required.

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.

Solution

Run the following commands to stop squid.service and remove the squid package:

systemctl stop squid.service # dnf remove 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

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b

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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lte rpm: squid-0.0.0-0

Hosts

10.74.6.135

```
The package 'squid-0.0.0-0' is not installed
```

2.2.18 Ensure web server services are not in use

Info

Web servers provide the ability to host web site content.

Rationale:

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.

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.

Solution

Run the following commands to stop httpd.socket, httpd.service, and nginx.service, and remove httpd and nginx packages:

systemctl stop httpd.socket httpd.service nginx.service # dnf remove httpd nginx

-OR-

-IF- a package is installed and is required for dependencies:

Run the following commands to stop and mask httpd.socket, httpd.service, and nginx.service:

systemctl stop httpd.socket httpd.service nginx.service # systemctl mask httpd.socket httpd.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.

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - nginx services exist on the system
The package 'nginx-0.0.0-0' is not installed

-------------------------
PASSED - httpd services exist on the system
The package 'httpd-0.0.0-0' is not installed
```

2.2.19 Ensure xinetd services are not in use

Info

The X Window System provides a Graphical User Interface (GUI) where users can have multiple windows in which to run programs and various add on. The X Windows system is typically used on workstations where users login, but not on servers where users typically do not login.

Rationale:

Unless your organization specifically requires graphical login access via X Windows, remove it to reduce the potential attack surface.

Impact:

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 the avahi-daemon.socket and avahi-daemon.service leaving the avahi package installed.

Solution

Run the following commands to stop xinetd.service, and remove the xinetd package:

systemctl stop xinetd.service # dnf remove 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

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lte rpm: xinetd-0.0.0-0

Hosts

10.74.6.135

```
The package 'xinetd-0.0.0-0' is not installed
```

2.2.21 Ensure mail transfer agents are 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.

Rationale:

The software for all Mail Transfer Agents is complex and most have a long history of security issues. While it is important to ensure that the system can process local mail messages, it is not necessary to have the MTA's daemon listening on a port unless the server is intended to be a mail server that receives and processes mail from other systems.

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 remediation is designed around the postfix mail server.

Depending on your environment you may have an alternative MTA installed such as sendmail. If this is the case consult the documentation for your installed MTA to configure the recommended state.

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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

GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - Loopback on Port 25
The command '/sbin/ss -plntu | /bin/grep -P -- ':25\b' | /bin/grep -Pv -- '\h*(127\.0\.0\.1|
\[?::1\]?):25\b' | /bin/awk -F: '{ print $NF } END {if (NR == 0) print "none"}'' returned :

none

-------------------------
PASSED - Loopback on Port 587
The command '/sbin/ss -plntu | /bin/grep -P -- ':587\b' | /bin/grep -Pv -- '\h*(127\.0\.0\.1|
\[?::1\]?):587\b' | /bin/awk -F: '{ print $NF } END {if (NR == 0) print "none"}'' returned :

none

-------------------------
PASSED - Loopback on Port 465
The command '/sbin/ss -plntu | /bin/grep -P -- ':465\b' | /bin/grep -Pv -- '\h*(127\.0\.0\.1|
\[?::1\]?):465\b' | /bin/awk -F: '{ print $NF } END {if (NR == 0) print "none"}'' returned :

none
```

2.3.1 Ensure ftp client is not installed

Info

FTP (File Transfer Protocol) is a traditional and widely used standard tool for transferring files between a server and clients over a network, especially where no authentication is necessary (permits anonymous users to connect to a server).

Rationale:

FTP does not protect the confidentiality of data or authentication credentials. It is recommended SFTP be used if file transfer is required. Unless there is a need to run the system as a FTP server (for example, to allow anonymous downloads), it is recommended that the package be removed to reduce the potential attack surface.

Solution

Run the following command to remove ftp:

dnf remove ftp

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lte rpm: ftp-0.0.0-0

Hosts

10.74.6.135

```
The package 'ftp-0.0.0-0' is not installed
```

2.3.3 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 (ypbind) was used to bind a machine to an NIS server and receive the distributed configuration files.

Rationale:

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed.

Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

Solution

Run the following command to remove the ypbind package:

dnf remove ypbind

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A

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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lte rpm: ypbind-0.0.0-0

Hosts

10.74.6.135

```
The package 'ypbind-0.0.0-0' is not installed
```

2.3.4 Ensure telnet client is not installed

Info

The telnet package contains the telnet client, which allows users to start connections to other systems via the telnet protocol.

Rationale:

The telnet protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow an unauthorized user to steal credentials. The ssh package provides an encrypted session and stronger security and is included in most Linux distributions.

Impact:

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

Solution

Run the following command to remove the telnet package:

dnf remove telnet

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a

PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lte rpm: telnet-0.0.0-0

Hosts

10.74.6.135

```
The package 'telnet-0.0.0-0' is not installed
```

2.3.5 Ensure tftp client is not installed

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.

Rationale:

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 command to remove tftp:

dnf remove tftp

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lte rpm: tftp-0.0.0-0

Hosts

10.74.6.135

```
The package 'tftp-0.0.0-0' is not installed
```

3.1.2 Ensure wireless interfaces are disabled

Info

Wireless networking is used when wired networks are unavailable.

Rationale:

-IF- wireless is not to be used, wireless devices can be disabled to reduce the potential attack surface.

Impact:

Many if not all laptop workstations and some desktop workstations will connect via wireless requiring these interfaces be enabled.

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 }

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$ timeout: 7200

Hosts

10.74.6.135

```
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.

Rationale:

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.

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.

Solution

Run the following commands to stop bluetooth.service, and remove the bluez package:

systemctl stop bluetooth.service # dnf remove 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

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
LEVEL	2A
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: lte rpm: bluez-0.0.0-0

Hosts

10.74.6.135

```
The package 'bluez-0.0.0-0' is not installed
```

3.4.1.1 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.

Rationale:

nftables is a subsystem of the Linux kernel that can protect against threats originating from within a corporate network to include malicious mobile code and poorly configured software on a host.

Impact:

Changing firewall settings while connected over the network can result in being locked out of the system.

Solution

Run the following command to install nftables

dnf install nftables

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: gt required: YES rpm: nftables-0.0.0-0

Hosts

10.74.6.135

```
The local RPM is newer than nftables-0.0.0-0 (nftables-1.0.4-4.el8_9)
```

3.4.1.2 Ensure a single firewall configuration utility is in use

Info

FirewallD - Is a firewall service daemon that provides a dynamic customizable host-based firewall with a D-Bus interface. Being dynamic, it enables creating, changing, and deleting the rules without the necessity to restart the firewall daemon each time the rules are changed

NFTables - Includes the nft utility for configuration of the nftables subsystem of the Linux kernel

Note: firewalld with nftables backend does not support passing custom nftables rules to firewalld, using the --direct option.

Rationale:

In order to configure firewall rules for nftables, a firewall utility needs to be installed and active of the system. The use of more than one firewall utility may produce unexpected results.

Solution

Run the following script to ensure that a single firewall utility is in use on the system:

#!/usr/bin/env bash

{ l_output='' l_output2='' l_fwd_status='' l_nft_status='' l_fwutil_status=''

Determine FirewallD utility Status rpm -q firewalld > /dev/null 2>&1 && l_fwd_status='$(systemctl is-enabled firewalld.service):$(systemctl is-active firewalld.service)'

Determine NFTables utility Status rpm -q nftables > /dev/null 2>&1 && l_nft_status='$(systemctl is-enabled nftables.service):$(systemctl is-active nftables.service)'

l_fwutil_status='$l_fwd_status:$l_nft_status'

case $l_fwutil_status in enabled:active:masked:inactive|enabled:active:disabled:inactive) echo -e '

- FirewallD utility is in use, enabled and active

- NFTables utility is correctly disabled or masked and inactive

- no remediation required' ;;

masked:inactive:enabled:active|disabled:inactive:enabled:active) echo -e '

- NFTables utility is in use, enabled and active

- FirewallD utility is correctly disabled or masked and inactive

- no remediation required' ;;

enabled:active:enabled:active) echo -e '

- Both FirewallD and NFTables utilities are enabled and active

- stopping and masking NFTables utility'

systemctl stop nftables && systemctl --now mask nftables ;;

enabled:*:enabled:*) echo -e '

- Both FirewallD and NFTables utilities are enabled

- remediating'

if ['$(awk -F: '{print $2}' <<< '$l_fwutil_status')' = 'active'] && ['$(awk -F: '{print $4}' <<< '$l_fwutil_status')' = 'inactive']; then echo ' - masking NFTables utility'

systemctl stop nftables && systemctl --now mask nftables elif ['$(awk -F: '{print $4}' <<< '$l_fwutil_status')' = 'active'] && ['$(awk -F: '{print $2}' <<< '$l_fwutil_status')' = 'inactive']; then echo ' - masking FirewallD utility'

systemctl stop firewalld && systemctl --now mask firewalld fi ;;

:active::active) echo -e '

- Both FirewallD and NFTables utilities are active

- remediating'

if ['$(awk -F: '{print $1}' <<< '$l_fwutil_status')' = 'enabled'] && ['$(awk -F: '{print $3}' <<< '$l_fwutil_status')' != 'enabled']; then echo ' - stopping and masking NFTables utility'

systemctl stop nftables && systemctl --now mask nftables elif ['$(awk -F: '{print $3}' <<< '$l_fwutil_status')' = 'enabled'] && ['$(awk -F: '{print $1}' <<< '$l_fwutil_status')' != 'enabled']; then echo ' - stopping and masking FirewallD utility'

systemctl stop firewalld && systemctl --now mask firewalld fi ;;

:enabled:active) echo -e '

- NFTables utility is in use, enabled, and active

- FirewallD package is not installed

- no remediation required' ;;

:) echo -e '

- Neither FirewallD or NFTables is installed.

- remediating

- installing NFTables'

dnf -q install nftables ;;

::) echo -e '

- NFTables package is not installed on the system

- remediating

- installing NFTables'

dnf -q install nftables ;;

*) echo -e '

- Unable to determine firewall state' ;;

esac }

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

- Audit Results:
 ** Pass **

 - FirewallD utility is in use, enabled and active
 - NFTables utility is correctly disabled or masked and inactive
```

3.4.2.3 Ensure firewalld drops unnecessary services and ports

Info

Services and ports can be accepted or explicitly rejected or dropped by a zone.

For every zone, you can set a default behavior that handles incoming traffic that is not further specified. Such behavior is defined by setting the target of the zone. There are three options - default, ACCEPT, REJECT, and DROP.

ACCEPT - you accept all incoming packets except those disabled by a specific rule.

REJECT - you disable all incoming packets except those that you have allowed in specific rules and the source machine is informed about the rejection.

DROP - you disable all incoming packets except those that you have allowed in specific rules and no information sent to the source machine.

Rationale:

To reduce the attack surface of a system, all services and ports should be blocked unless required

Solution

If Firewalld is in use on the system:

Run the following command to remove an unnecessary service:

firewall-cmd --remove-service=<service>

Example:

firewall-cmd --remove-service=cockpit

Run the following command to remove an unnecessary port:

firewall-cmd --remove-port=<port-number>/<port-type>

Example:

firewall-cmd --remove-port=25/tcp

Run the following command to make new settings persistent:

firewall-cmd --runtime-to-permanent

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.13.1
800-171	3.13.5

800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

3.4.2.4 Ensure nftables established connections are configured

Info

Configure the firewall rules for new outbound and established connections

Rationale:

If rules are not in place for established connections, all packets will be dropped by the default policy preventing network usage.

Solution

If NFTables utility is in use on your system:

Configure nftables in accordance with site policy. The following commands will implement a policy to allow all established connections:

systemctl is-enabled nftables.service | grep -q 'enabled' && nft add rule inet filter input ip protocol tcp ct state established accept # systemctl is-enabled nftables.service | grep -q 'enabled' && nft add rule inet filter input ip protocol udp ct state established accept # systemctl is-enabled nftables.service | grep -q 'enabled' && nft add rule inet filter input ip protocol icmp ct state established accept

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b

GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

3.4.2.5 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.

Rationale:

There are two policies: accept (Default) and drop. If the policy is set to accept, the firewall will accept any packet that is not configured to be denied and the packet will continue traversing the network stack.

It is easier to explicitly permit acceptable usage than to deny unacceptable usage.

Note: Changing firewall settings while connected over the network can result in being locked out of the system.

Impact:

If configuring nftables over ssh, creating a base chain with a policy of drop will cause loss of connectivity.

Ensure that a rule allowing ssh has been added to the base chain prior to setting the base chain's policy to drop

Solution

If NFTables utility is in use on your system:

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 ; }

Default Value:

accept

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.13.1
800-171	3.13.5
800-171	3.13.6
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
GDPR	32.1.b
GDPR	32.1.d
GDPR	32.2
HIPAA	164.306(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

4.1.1.1 Ensure cron daemon is enabled and active

Info

The cron daemon is used to execute batch jobs on the system.

Rationale:

While there may not be user jobs that need to be run on the system, the system does have maintenance jobs that may include security monitoring that have to run, and cron is used to execute them.

Solution

- IF - cron is installed on the system:

Run the following commands to unmask, enable, and start crond:

systemctl unmask crond # systemctl --now enable crond

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-53	CM-6b.
800-53R5	CM-6b.
CN-L3	8.1.10.6(d)
CSF	PR.IP-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6b.
LEVEL	1A
NESA	T3.2.1
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

------------------------
PASSED - cron daemon is enabled
The command '/bin/systemctl is-enabled crond' returned :

enabled

------------------------
PASSED - cron daemon is active
The command '/bin/systemctl is-active crond' returned :

active
```

4.1.1.2 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.

Rationale:

This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

Solution

Run the following commands to set ownership and permissions on /etc/crontab:

chown root:root /etc/crontab # chmod og-rwx /etc/crontab

Default Value:

Access: (644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

file: /etc/crontab group: root mask: 177 owner: root

Hosts

10.74.6.135

```
The file /etc/crontab with fmode owner: root group: root mode: 0600 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/crontab
```

4.1.1.3 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.

Rationale:

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

Solution

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/

Default Value:

Access: (755/drwxr-xr-x) Uid: (0/ root) Gid: (0/ root)

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

file: /etc/cron.hourly group: root mask: 077 owner: root

Hosts

10.74.6.135

```
The file /etc/cron.hourly with fmode owner: root group: root mode: 0700 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/cron.hourly
```

4.1.1.4 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.

Rationale:

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

Solution

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/

Default Value:

Access: (755/drwxr-xr-x) Uid: (0/ root) Gid: (0/ root)

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

file: /etc/cron.daily group: root mask: 077 owner: root

Hosts

10.74.6.135

```
The file /etc/cron.daily with fmode owner: root group: root mode: 0700 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/cron.daily
```

4.1.1.5 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.

Rationale:

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

Solution

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/

Default Value:

Access: (755/drwxr-xr-x) Uid: (0/ root) Gid: (0/ root)

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

file: /etc/cron.weekly group: root mask: 077 owner: root

Hosts

10.74.6.135

```
The file /etc/cron.weekly with fmode owner: root group: root mode: 0700 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/cron.weekly
```

4.1.1.6 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.

Rationale:

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

Solution

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/

Default Value:

Access: (755/drwxr-xr-x) Uid: (0/ root) Gid: (0/ root)

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

file: /etc/cron.monthly group: root mask: 077 owner: root

Hosts

10.74.6.135

```
The file /etc/cron.monthly with fmode owner: root group: root mode: 0700 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/cron.monthly
```

4.1.1.7 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.

Rationale:

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

Solution

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/

Default Value:

Access: (755/drwxr-xr-x) Uid: (0/ root) Gid: (0/ root)

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

file: /etc/cron.d group: root mask: 077 owner: root

Hosts

10.74.6.135

```
The file /etc/cron.d with fmode owner: root group: root mode: 0700 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/cron.d
```

4.1.1.8 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

Rationale:

On many systems, only the system administrator is authorized to schedule cron jobs. Using the cron.allow file to control who can run cron jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Solution

-IF- cron is installed on the system:

Run the following commands to:

Create /etc/cron.allow if it doesn't exist

Change owner or user root

Change group owner to group root

Change mode to 640 or more restrictive

[! -e '/etc/cron.allow'] && touch /etc/cron.allow # chown root:root /etc/cron.allow # chmod u-x,g-wx,o-rwx /etc/cron.allow

Run the following commands to:

-IF- /etc/cron.deny exists:

Change owner or user root

Change group owner to group root

Change mode to 640 or more restrictive

[-e '/etc/cron.deny'] && chown root:root /etc/cron.deny # [-e '/etc/cron.deny'] && chmod u-x,g-wx,o-rwx /etc/cron.deny

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

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


-------------------------
PASSED - /etc/cron.allow file permissions
The file /etc/cron.allow with fmode owner: root group: root mode: 0600 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/cron.allow
```

4.1.2.1 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.

Rationale:

On many systems, only the system administrator is authorized to schedule at jobs. Using the at.allow file to control who can run at jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

4.2.1 Ensure permissions on /etc/ssh/sshd_config are configured

Info

The file /etc/ssh/sshd_config, and files ending in .conf in the /etc/ssh/sshd_config.d directory, contain configuration specifications for sshd.

Rationale:

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 in .conf 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) }

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$ timeout: 7200

Hosts

10.74.6.135

```
The command script with multiple lines returned :

find: '/etc/ssh/sshd_config.d': No such file or directory

- Audit Result:
  *** PASS ***
- * Correctly set * :

 - File: "/etc/ssh/sshd_config":
  - Correct: mode (0600), owner (root), and group owner (root) configured
```

4.2.3 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.

Rationale:

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

{ l_output='' l_output2=''

l_skgn='$(grep -Po -- '^(ssh_keys|_?ssh)b' /etc/group)' # Group designated to own openSSH keys
l_skgid='$(awk -F: '($1 == "'$l_skgn'"){print $3}' /etc/group)' # Get gid of group l_mfix='u-x,go-wx'

unset a_skarr && a_skarr=() # Clear and initialize array if [ -d /etc/ssh ]; then while IFS= read -r -d $'0' l_file; do # Loop to populate array if grep -Pq ':h+OpenSSHh+(H+h+)publich+keyb' <<< '$(file '$l_file')'; then a_skarr+=('$(stat -Lc '%n^%#a^%U^%G^%g' '$l_file')') fi done < <(find -L /etc/ssh -xdev -type f -print0) while IFS='^' read -r l_file l_mode l_owner l_group l_gid; do l_out2=''

l_pmask='0133'

l_maxperm='$( printf '%o' $(( 0777 & ~$l_pmask )) )'

if [ $(( $l_mode & $l_pmask )) -gt 0 ]; then l_out2='$l_out2

- Mode: '$l_mode' should be mode: '$l_maxperm' or more restrictive

- Revoking excess permissions'

chmod '$l_mfix' '$l_file'

fi if [ '$l_owner' != 'root' ]; then l_out2='$l_out2

- Owned by: '$l_owner' should be owned by 'root'

- Changing ownership to 'root''

chown root '$l_file'

fi if [[ ! '$l_group' =~ $l_agroup ]]; then l_out2='$l_out2

- Owned by group '$l_group' should be group owned by: '${l_agroup//|/ or }'

- Changing group ownership to '$l_sgroup''

chgrp '$l_sgroup' '$l_file'

fi [ -n '$l_out2' ] && l_output2='$l_output2

- File: '$l_file'$l_out2'

done <<< '$(printf '%s ' '${a_skarr[@]}')'

else l_output=' - openSSH keys not found on the system'

fi unset a_skarr if [ -z '$l_output2' ]; then echo -e '

- No access changes required '
```

else echo -e '
- Remediation results:
$l_output2 '
fi }

Default Value:

644 0/root 0/root

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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	5.1
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
GDPR	32.1.b

HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$ timeout: 7200

Hosts

10.74.6.135

```
The command script with multiple lines returned :

File: "/etc/ssh/ssh_host_rsa_key.pub" Mode: "0644" Owner: "root" Group: "root" GID: "0"
File: "/etc/ssh/ssh_host_ecdsa_key.pub" Mode: "0644" Owner: "root" Group: "root" GID: "0"
File: "/etc/ssh/ssh_host_ed25519_key.pub" Mode: "0644" Owner: "root" Group: "root" GID: "0"

- Audit Result:
  *** PASS ***
- * Correctly set * :

 - 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
 - File: "/etc/ssh/ssh_host_ed25519_key.pub"
  - Correct: mode (0644), owner (root), and group owner (root) configured
```

4.2.6 Ensure sshd Ciphers are configured

Info

This variable limits the ciphers that SSH can use during communication.

Note:

Some organizations may have stricter requirements for approved ciphers.

Ensure that ciphers used are in compliance with site policy.

The only 'strong' ciphers currently FIPS 140-2 compliant are:

aes256-ctr

aes192-ctr

aes128-ctr

Rationale:

Weak ciphers that are used for authentication to the cryptographic module cannot be relied upon to provide confidentiality or integrity, and system data may be compromised.

The 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.

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,rijndael-cbc@lysator.liu.se

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.

Default Value:

Ciphers chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.13
800-171	3.5.2
800-171	3.13.8
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
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/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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Pass$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

/etc/ssh/sshd_config: Permission denied
port 22:
Pass
```

4.2.11 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 140-2 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

Rationale:

Key exchange methods that are considered weak should be removed. A key exchange method may be weak because too few bits are used, or the hashing algorithm is considered too weak. Using weak algorithms could expose connections to man-in-the-middle attacks

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.

Default Value:

KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.13
800-171	3.5.2
800-171	3.13.8
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
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/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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Pass$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

/etc/ssh/sshd_config: Permission denied
port 22:
Pass
```

4.2.14 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 140-2 approved are:

HMAC-SHA1

HMAC-SHA2-256

HMAC-SHA2-384

HMAC-SHA2-512

Rationale:

MD5 and 96-bit MAC algorithms are considered weak and have been shown to increase exploitability in SSH downgrade attacks. Weak algorithms continue to have a great deal of attention as a weak spot that can be exploited with expanded computing power. An attacker that breaks the algorithm could take advantage of a MiTM position to decrypt the SSH tunnel and capture credentials and information.

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

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.

The default is handled system-wide by crypto-policies(7). Information about defaults, how to modify the defaults and how to customize existing policies with sub-policies are present in manual page update-crypto-policies(8)

Default Value:

MACs umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.13
800-171	3.5.2
800-171	3.13.8
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
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/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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: ^Pass$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

/etc/ssh/sshd_config: Permission denied
port 22:
Pass
```

4.3.1 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.

Rationale:

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

Run the following command to install sudo

dnf install sudo

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.5
800-171	3.1.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)

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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: gt required: YES rpm: sudo-0.0.0-0

Hosts

10.74.6.135

```
The local RPM is newer than sudo-0.0.0-0 (sudo-1.9.5p2-1.el8_9)
```

4.3.6 Ensure sudo authentication timeout is configured correctly

Info

sudo caches used credentials for a default of 5 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.

Rationale:

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 its 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/15289

References

800-171	3.1.5
800-171	3.1.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
FAILED - sudo timeout
The command '/bin/sudo -V | /bin/grep 'Authentication timestamp timeout:'' did not return any result

-------------------------
PASSED - On disk timestamp_timeout
No matching files were found
```

4.3.7 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.

Rationale:

Restricting the use of su , and using sudo in its place, provides system administrators better control of the escalation of user privileges to execute privileged commands. The sudo utility also provides a better logging and audit mechanism, as it can log each command executed via sudo , whereas su can only record that a user executed the su program.

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/15289

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
800-53	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	5.1
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: sugroup=$(/bin/grep -Pi '^\h*auth\h+(?:required|requisite)\h+pam_wheel\.so\h+(?:[^# \r]+\h+)?((?!\2)(use_uid\b|group=\H+\b))\h+(?:[^# \r]+\h+)?((?!\1)(use_uid\b|group=\H+\b))(\h+.*)?$' /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 expect: pass - group empty

Hosts

10.74.6.135

```
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 :

pass - group empty
```

4.4.1.1 Ensure latest version of pam is installed

Info

Updated versions of PAM include additional functionality

Rationale:

To ensure the system has full functionality and access to the options covered by this Benchmark, pam-1.3.1-25 or latter is required

Solution

- IF - the version of PAM on the system is less that version pam-1.3.1-25:

Run the following command to update to the latest version of PAM:

dnf upgrade pam

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.1
800-53	IA-2(11)
800-53R5	IA-2(6)
CN-L3	8.1.4.1(d)
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-2(100)
LEVEL	1A
NESA	T5.4.2
NIAV2	AM2
NIAV2	AM8
NIAV2	AM14b
PCI-DSSV3.2.1	8.3
PCI-DSSV3.2.1	8.3.1
PCI-DSSV3.2.1	8.3.2
PCI-DSSV4.0	8.4.1
PCI-DSSV4.0	8.4.3
QCSC-V1	5.2.2
QCSC-V1	13.2

SWIFT-CSCV1	4.2
TBA-FIISB	35.1
TBA-FIISB	36.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: gte rpm: pam-1.3.1-25

Hosts

10.74.6.135

```
The local RPM is newer than pam-1.3.1-25 (pam-1.3.1-27.0.1.el8)
```

4.4.1.2 Ensure latest version of authselect is installed

Info

Authselect is a utility that simplifies the configuration of user authentication. Authselect offers ready-made profiles that can be universally used with all modern identity management systems

You can create and deploy a custom profile by customizing one of the default profiles, the sssd, winbind, or the nis profile. This is particularly useful if Modifying a ready-made authselect profile is not enough for your needs. When you deploy a custom profile, the profile is applied to every user logging into the given host. This would be the recommended method, so that the existing profiles can remain unmodified.

Updated versions of authselect include additional functionality

Rationale:

Authselect makes testing and troubleshooting easy because it only modifies files in these directories:

/etc/nsswitch.conf

/etc/pam.d/*

/etc/dconf/db/distro.d/*

To ensure the system has full functionality and access to the options covered by this Benchmark, authselect-1.2.6-1 or latter is required

Impact:

If local site customizations have been made to an authselect default or custom profile created with the --symlink-pam option, these customizations may be over-written by updating authselect.

WARNING:

Do not use authselect if:

your host is part of Linux Identity Management. Joining your host to an IdM domain with the ipa-client-install command automatically configures SSSD authentication on your host.

Your host is part of Active Directory via SSSD. Calling the realm join command to join your host to an Active Directory domain automatically configures SSSD authentication on your host.

It is not recommended to change the authselect profiles configured by ipa-client-install or realm join. If you need to modify them, display the current settings before making any modifications, so you can revert back to them if necessary

Solution

Run the following command to install authselect:

dnf install authselect

- IF - the version of authselect on the system is less that version authselect-1.2.6-1:

Run the following command to update to the latest version of authselect:

dnf upgrade authselect

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.8
800-53	AC-7a.
800-53R5	AC-7a.
CN-L3	8.1.4.1(b)
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	AC-7a.
LEVEL	1A
NESA	T5.5.1
NIAV2	AM24
PCI-DSSV3.2.1	8.1.6
PCI-DSSV4.0	8.3.4
TBA-FIISB	45.1.2
TBA-FIISB	45.2.1
TBA-FIISB	45.2.2

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: gte rpm: authselect-1.2.6-1

Hosts

10.74.6.135

```
The local RPM is newer than authselect-1.2.6-1 (authselect-1.2.6-2.el8)
```

4.4.2.3 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.

Rationale:

Use of a unique, complex passwords helps to increase the time and resources required to compromise the password.

Solution

Review the authselect profile templates:

Run the following script to verify the pam_pwquality.so lines exist in the active profile templates:

#!/usr/bin/env bash

{ l_module_name='pwquality'

l_pam_profile='$(head -1 /etc/authselect/authselect.conf)'

if grep -Pq -- '^custom/' <<< '$l_pam_profile'; then l_pam_profile_path='/etc/authselect/$l_pam_profile'

else l_pam_profile_path='/usr/share/authselect/default/$l_pam_profile'

fi grep -P -- 'bpam_$l_module_name.sob' '$l_pam_profile_path'/{password,system}-auth }

Example Output with a custom profile named 'custom-profile':

/etc/authselect/custom/custom-profile/password-auth:password requisite pam_pwquality.so local_users_only {include if 'with-pwquality'}

/etc/authselect/custom/custom-profile/system-auth:password requisite pam_pwquality.so local_users_only {include if 'with-pwquality'}

Note: The lines may not include {include if 'with-pwquality'}

- IF - the lines shown above are not returned, refer to the Recommendation 'Ensure active authselect profile includes pam modules' to update the authselect profile template files to include the pam_pwquality entries before continuing this remediation.

- IF - any of the pam_pwquality lines include {include if 'with-pwquality'}, run the following command to enable the authselect with-pwquality feature and update the files in /etc/pam.d to include 'pam_pwquality:

authselect enable-feature with-pwquality

- IF - any of the pam_pwquality lines exist without {include if 'with-pwquality'}, run the following command to update the files in /etc/pam.d to include pam_pwquality.so:

authselect apply-changes

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - Ensure at least one file named /etc/pam.d/system-auth exists and matches pattern ^h*authh
+(required|requisite)h+([^#r
]+h+)?pam_faillock.soh+([^#r
]+h+)?authfailb
Compliant file(s):
      /etc/pam.d/system-auth - regex '(?i)^\h*password\h+(requisite|required)\h+pam_pwquality\.so
\b' found - expect '(?i)^\h*password\h+(requisite|required)\h+pam_pwquality\.so\b' found in the
 following lines:
          19: password    requisite                                     pam_pwquality.so
 try_first_pass local_users_only enforce_for_root retry=3
```

```
-------------------------
PASSED - Ensure at least one file named /etc/pam.d/password-auth exists and matches pattern (?
i)^h*passwordh+(requisite|required)h+pam_pwquality.sob
Compliant file(s):
      /etc/pam.d/password-auth - regex '(?i)^\h*password\h+(requisite|required)\h+pam_pwquality\.so
\b' found - expect '(?i)^\h*password\h+(requisite|required)\h+pam_pwquality\.so\b' found in the
 following lines:
          19: password    requisite                                     pam_pwquality.so
 try_first_pass local_users_only enforce_for_root retry=3
```

4.4.2.5 Ensure pam_unix module is enabled

Info

The pam_unix.so module 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 the /etc/shadow file as well if shadow is enabled.

Rationale:

Requiring users to use authentication make it less likely that an attacker will be able to access the system.

Solution

Run the following script to verify the pam_unix.so lines exist in the profile templates:

#!/usr/bin/env bash

{ l_module_name='unix'

l_pam_profile='$(head -1 /etc/authselect/authselect.conf)'

if grep -Pq -- '^custom/' <<< '$l_pam_profile'; then l_pam_profile_path='/etc/authselect/$l_pam_profile'

else l_pam_profile_path='/usr/share/authselect/default/$l_pam_profile'

fi grep -P -- 'bpam_$l_module_name.sob' '$l_pam_profile_path'/{password,system}-auth }

Example Output with a custom profile named 'custom-profile':

/etc/authselect/custom/custom-profile/password-auth:auth sufficient pam_unix.so {if not 'without-nullok':nullok} /etc/authselect/custom/custom-profile/password-auth:account required pam_unix.so /etc/authselect/custom/custom-profile/password-auth:password sufficient pam_unix.so sha512 shadow {if not 'without-nullok':nullok} use_authtok remember=5 /etc/authselect/custom/custom-profile/password-auth:session required pam_unix.so

/etc/authselect/custom/custom-profile/system-auth:auth sufficient pam_unix.so {if not 'without-nullok':nullok} /etc/authselect/custom/custom-profile/system-auth:account required pam_unix.so /etc/authselect/custom/custom-profile/system-auth:password sufficient pam_unix.so sha512 shadow {if not 'without-nullok':nullok} use_authtok /etc/authselect/custom/custom-profile/system-auth:session required pam_unix.so

- IF - the lines shown above are not returned, refer to the Recommendation 'Ensure active authselect profile includes pam modules' to update the authselect profile template files to include the pam_unix entries before continuing this remediation.

Note: Arguments following pam_unix.so may be different than the example output

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.1
800-53	IA-2

800-53R5	IA-2
CN-L3	7.1.3.1(a)
CN-L3	7.1.3.1(e)
CN-L3	8.1.4.1(a)
CN-L3	8.1.4.2(a)
CN-L3	8.5.4.1(a)
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-2
ITSG-33	IA-2a.
LEVEL	1A
NESA	T2.3.8
NESA	T5.3.1
NESA	T5.4.2
NESA	T5.5.1
NESA	T5.5.2
NESA	T5.5.3
NIAV2	AM2
NIAV2	AM8
NIAV2	AM14b
QCSC-V1	5.2.2
QCSC-V1	13.2
TBA-FIISB	35.1
TBA-FIISB	36.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - Ensure at least one file named /etc/pam.d/system-auth exists and matches auth pattern
Compliant file(s):
```

```
      /etc/pam.d/system-auth - regex '^\h*auth\h+(required|requisite|sufficient)\h+pam_unix\.so\b'
 found - expect '^\h*auth\h+(required|requisite|sufficient)\h+pam_unix\.so\b' found in the following
 lines:
          8: auth        sufficient    pam_unix.so try_first_pass

-------------------------
PASSED - Ensure at least one file named /etc/pam.d/system-auth exists and matches account pattern
Compliant file(s):
      /etc/pam.d/system-auth - regex '^\h*password\h+(required|requisite|sufficient)\h+pam_unix\.so
\b' found - expect '^\h*password\h+(required|requisite|sufficient)\h+pam_unix\.so\b' found in the
 following lines:
          22: password    sufficient                                    pam_unix.so sha512 shadow
 try_first_pass use_authtok remember=5

-------------------------
PASSED - Ensure at least one file named /etc/pam.d/password-auth exists and matches account pattern
Compliant file(s):
      /etc/pam.d/password-auth - regex '^\h*account\h+(required|requisite)\h+pam_unix\.so\b' found -
 expect '^\h*account\h+(required|requisite)\h+pam_unix\.so\b' found in the following lines:
          13: account     required      pam_unix.so

-------------------------
PASSED - Ensure at least one file named /etc/pam.d/system-auth exists and matches account pattern
Compliant file(s):
      /etc/pam.d/system-auth - regex '^\h*account\h+(required|requisite)\h+pam_unix\.so\b' found -
 expect '^\h*account\h+(required|requisite)\h+pam_unix\.so\b' found in the following lines:
          13: account     required      pam_unix.so

-------------------------
PASSED - Ensure at least one file named /etc/pam.d/password-auth exists and matches session pattern
Compliant file(s):
      /etc/pam.d/password-auth - regex '^\h*session\h+(required|requisite)\h+pam_unix\.so\b' found -
 expect '^\h*session\h+(required|requisite)\h+pam_unix\.so\b' [...]
```

4.4.3.1.1 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 .

Rationale:

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 script to remove the deny argument from the pam_faillock.so module in the PAM files:

#!/usr/bin/env bash { for l_pam_file in system-auth password-auth; do l_authselect_file='/etc/authselect/$(head -1 /etc/authselect/authselect.conf | grep 'custom/')/$l_pam_file'

sed -ri 's/(^s*auths+(requisite|required|sufficient)s+pam_faillock.so.*)(s+denys*=s*S+)(.*$)/14/' '$l_authselect_file'

done authselect apply-changes }

Default Value:

deny = 3

Additional Information:

If a user has been locked out because they have reached the maximum consecutive failure count defined by deny= in the pam_faillock.so module, the user can be unlocked by issuing the command faillock --user <USERNAME> --reset. This command sets the failed count to 0, effectively unlocking the user.

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.1
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

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

```
PASSED - Ensure the deny argument has not been set, or 5 or less and meets local site policy
No matching files were found

------------------------
PASSED - Ensure at least one file named /etc/security/faillock.conf exists and matches deny pattern
Compliant file(s):
      /etc/security/faillock.conf - regex '(?i)^\h*deny\h*=\h*[1-5]\b' found - expect '(?i)^\h*deny
\h*=\h*[1-5]\b' found in the following lines:
          63: deny = 5
```

4.4.3.1.2 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

Rationale:

Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

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.

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 script to remove the unlock_time argument from the pam_faillock.so module in the PAM files:

#!/usr/bin/env bash { for l_pam_file in system-auth password-auth; do l_authselect_file='/etc/authselect/$(head -1 /etc/authselect/authselect.conf | grep 'custom/')/$l_pam_file'

sed -ri 's/(^s*auths+(requisite|required|sufficient)s+pam_faillock.so.*)(s+unlock_times*=s*S+)(.*$)/14/' '$l_authselect_file'

done authselect apply-changes } ''

Default Value:

unlock_time = 600

Additional Information:

If a user has been locked out because they have reached the maximum consecutive failure count defined by deny= in the pam_faillock.so module, the user can be unlocked by issuing the command faillock --user <USERNAME> --reset. This command sets the failed count to 0, effectively unlocking the user.

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.1
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - Verify that the unlock_time argument has not been set, or is either 0 (never) or 900 (15
 minutes) or more and meets local site policy
No matching files were found

-------------------------
PASSED - Ensure at least one file named /etc/security/faillock.conf exists and matches unlock_time
 pattern
Compliant file(s):
      /etc/security/faillock.conf - regex '(?i)^\h*unlock_time\h*=' found - expect '(?i)^
\h*unlock_time\h*=\h*(0|9[0-9][0-9]|[1-9][0-9]{3,})\b' found in the following lines:
          64: unlock_time = 900
```

4.4.3.2.2 Ensure password length is configured

Info

minlen - 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.

Rationale:

Strong passwords protect systems from being hacked through brute force methods.

Solution

Create or modify a file ending in .conf 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:

sed -ri 's/^s*minlens*=/# &/' /etc/security/pwquality.conf # printf '

%s' 'minlen = 14' >> /etc/security/pwquality.conf.d/50-pwlength.conf

Run the following script to remove setting minlen on the pam_pwquality.so module in the PAM files:

#!/usr/bin/env bash

{ for l_pam_file in system-auth password-auth; do l_authselect_file='/etc/authselect/$(head -1 /etc/authselect/authselect.conf | grep 'custom/')/$l_pam_file'

sed -ri 's/(^s*passwords+(requisite|required|sufficient)s+pam_pwquality.so.*)(s+minlens*=s*[0-9]+)(.*$)/14/' '$l_authselect_file'

done authselect apply-changes }

Default Value:

minlen = 8

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - Verify that minlen is not set, or is 14 or more characters, and conforms to local site
 policy
No matching files were found

-------------------------
PASSED - Ensure at least one file named /etc/security/pwquality.conf exists and matches minlen
 pattern
Compliant file(s):
      /etc/security/pwquality.conf - regex '(?i)^\h*minlen\h*=' found - expect '(?i)^\h*minlen\h*=
\h*(1[4-9]|[2-9][0-9]|[1-9][0-9]{2,})\b' found in the following lines:
          51: minlen = 14
```

4.4.3.2.3 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

Rationale:

Strong passwords protect systems from being hacked through brute force methods.

Solution

Create or modify a file ending in .conf in the /etc/security/pwquality.conf.d/ directory or the file /etc/security/pwquality.conf and add or modify the following line to set:

minclass = 4

--AND/OR--

dcredit = -_N_

ucredit = -_N_

ocredit = -_N_

lcredit = -_N_

Example:

sed -ri 's/^s*minclasss*=/# &/' /etc/security/pwquality.conf # printf '

%s' 'minclass = 4' >> /etc/security/pwquality.conf.d/50-pwcomplexity.conf

--AND/OR--

sed -ri 's/^s*[dulo]credits*=/# &/' /etc/security/pwquality.conf # printf '%s ' 'dcredit = -1' 'ucredit = -1' 'ocredit = -1' 'lcredit = -1' > /etc/security/pwquality.conf.d/50-pwcomplexity.conf

Run the following script to remove setting minclass, dcredit, ucredit, lcredit, and ocredit on the pam_pwquality.so module in the PAM files

#!/usr/bin/env bash

{ for l_pam_file in system-auth password-auth; do l_authselect_file='/etc/authselect/$(head -1 /etc/authselect/authselect.conf | grep 'custom/')/$l_pam_file'

sed -ri 's/(^s*passwords+(requisite|required|sufficient)s+pam_pwquality.so.*)(s+minclasss*=s*S+)(.*$)/14/' '$l_authselect_file'

sed -ri 's/(^s*passwords+(requisite|required|sufficient)s+pam_pwquality.so.*)(s+dcredits*=s*S+)(.*$)/14/' '$l_authselect_file'

sed -ri 's/(^s*passwords+(requisite|required|sufficient)s+pam_pwquality.so.*)(s+ucredits*=s*S+)(.*$)/14/' '$l_authselect_file'

sed -ri 's/(^s*passwords+(requisite|required|sufficient)s+pam_pwquality.so.*)(s+lcredits*=s*S+)(.*$)/14/' '$l_authselect_file'

sed -ri 's/(^s*passwords+(requisite|required|sufficient)s+pam_pwquality.so.*)(s+ocredits*=s*S+)(.*$)/14/' '$l_authselect_file'

done authselect apply-changes }

Default Value:

minclass = 0

dcredit = 0

ucredit = 0

ocredit = 0

lcredit = 0

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1M
NESA	T5.2.3

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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: ^[\s]*minclass[\s]*=[\s]*4[\s]*$ file: /etc/security/pwquality.conf /etc/security/pwquality.conf.d/*.conf min_occurrences: 1 regex: ^[\s]*minclass[\s]*= string_required: NO

Hosts

10.74.6.135

```
Compliant file(s):
      /etc/security/pwquality.conf - regex '^[\s]*minclass[\s]*=' found - expect
 '^[\s]*minclass[\s]*=[\s]*4[\s]*$' found in the following lines:
          56: minclass = 4
```

4.4.3.2.6 Ensure password dictionary check is enabled

Info

The pwquality dictcheck option sets whether to check for the words from the cracklib dictionary.

Rationale:

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 in .conf 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 script to remove setting dictcheck on the pam_pwquality.so module in the PAM files:

#!/usr/bin/env bash

{ for l_pam_file in system-auth password-auth; do l_authselect_file='/etc/authselect/$(head -1 /etc/authselect/authselect.conf | grep 'custom/')/$l_pam_file'

sed -ri 's/(^s*passwords+(requisite|required|sufficient)s+pam_pwquality.so.*)(s+dictchecks*=s*S+)(.*$)/14/' '$l_authselect_file'

done authselect apply-changes }

Default Value:

dictcheck = 1

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)

HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - Verify that the dictcheck option is not set to 0 (disabled) in a pwquality configuration
 file
The file "/etc/security/pwquality.conf" does not contain "(?i)^\h*dictcheck\h*=\h*0\b"

-------------------------
PASSED - Verify that the dictcheck option is not set to 0 (disabled) as a module argument in a PAM
 file
The file "/etc/pam.d/password-auth" does not contain "(?i)^\h*password\h+(requisite|required|
sufficient)\h+pam_pwquality\.so\h+([^#\r]+\h+)?dictcheck\h*=\h*0\b"
```

4.4.3.4.1 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.

Rationale:

Using a strong password is essential to helping protect personal and sensitive information from unauthorized access

Solution

Run the following script to verify that the active authselect profile's system-auth and password-auth files include {if not 'without-nullok':nullok} - OR - don't include the nullok option on the pam_unix.so module:

{ l_module_name='unix'

l_profile_name='$(head -1 /etc/authselect/authselect.conf)'

if [[! '$l_profile_name' =~ ^custom/]]; then echo ' - Follow Recommendation 'Ensure custom authselect profile is used' and then return to this Recommendation'

else grep -P -- 'bpam_$l_module_name.sob' /etc/authselect/$l_profile_name/{password,system}-auth fi }

Example output with a custom profile named 'custom-profile':

/etc/authselect/custom/custom-profile/password-auth:auth sufficient pam_unix.so {if not 'without-nullok':nullok} /etc/authselect/custom/custom-profile/password-auth:account required pam_unix.so /etc/authselect/custom/custom-profile/password-auth:password sufficient pam_unix.so sha512 shadow {if not 'without-nullok':nullok} use_authtok /etc/authselect/custom/custom-profile/password-auth:session required pam_unix.so

/etc/authselect/custom/custom-profile/system-auth:auth sufficient pam_unix.so {if not 'without-nullok':nullok} /etc/authselect/custom/custom-profile/system-auth:account required pam_unix.so /etc/authselect/custom/custom-profile/system-auth:password sufficient pam_unix.so sha512 shadow {if not 'without-nullok':nullok} use_authtok /etc/authselect/custom/custom-profile/system-auth:session required pam_unix.so

- IF - any line is returned with nullok that doesn't also include {if not 'without-nullok':nullok}, run the following script:

#!/usr/bin/env bash

{ for l_pam_file in system-auth password-auth; do l_file='/etc/authselect/$(head -1 /etc/authselect/authselect.conf | grep 'custom/')/$l_pam_file'

sed -ri 's/(^s*passwords+(requisite|required|sufficient)s+pam_unix.sos+.*)(nullok)(s*.*)$/124/g' $l_file done }

- IF - any line is returned with {if not 'without-nullok':nullok}, run the following command to enable the authselect without-nullok feature:

authselect enable-feature without-nullok

Run the following command to update the files in /etc/pam.d to include pam_unix.so without the nullok argument:

authselect apply-changes

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - Ensure no file named /etc/pam.d/password-auth exists and matches pattern
The file "/etc/pam.d/password-auth" does not contain "(?i)^\h*(auth|account|password|session)\h
+(requisite|required|sufficient)\h+pam_unix\.so\h+([^#\n\r]+\h+)?nullok\b"

-------------------------
PASSED - Ensure no file named /etc/pam.d/system-auth exists and matches pattern
The file "/etc/pam.d/system-auth" does not contain "(?i)^\h*(auth|account|password|session)\h
+(requisite|required|sufficient)\h+pam_unix\.so\h+([^#\n\r]+\h+)?nullok\b"
```

4.4.3.4.3 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.

Rationale:

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

Note:

If yescrypt becomes available in a future release, this would also be acceptable. It is highly recommended that the chosen hashing algorithm is consistent across /etc/libuser.conf, /etc/login.defs, /etc/pam.d/password-auth, and /etc/pam.d/system-auth.

This only effects local users and passwords created after updating the files 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 user ID's be immediately expired and forced to change their passwords on next login.

Run the following script to verify the active authselect profile includes a strong password hashing algorithm on the password stack's pam_unix.so module lines:

#!/usr/bin/env bash

{ l_pam_profile='$(head -1 /etc/authselect/authselect.conf)'

if grep -Pq -- '^custom/' <<< '$l_pam_profile'; then l_pam_profile_path='/etc/authselect/$l_pam_profile'

else l_pam_profile_path='/usr/share/authselect/default/$l_pam_profile'

fi grep -P -- '^h*passwordh+(requisite|required|sufficient)h+pam_unix.soh+([^# r]+h+)?(sha512|yescrypt)b' '$l_pam_profile_path'/{password,system}-auth }

Example output:

/etc/authselect/custom/custom-profile/password-auth:password sufficient pam_unix.so sha512 shadow {if not 'without-nullok':nullok} use_authtok

/etc/authselect/custom/custom-profile/system-auth:password sufficient pam_unix.so sha512 shadow {if not 'without-nullok':nullok} use_authtok

- IF - the output does not include either sha512 - OR - yescrypt, or includes a different hashing algorithm, run the following script:

#!/usr/bin/env bash

{ l_pam_profile='$(head -1 /etc/authselect/authselect.conf)'

if grep -Pq -- '^custom/' <<< '$l_pam_profile'; then l_pam_profile_path='/etc/authselect/$l_pam_profile'

else l_pam_profile_path='/usr/share/authselect/default/$l_pam_profile'

fi for l_authselect_file in '$l_pam_profile_path'/password-auth '$l_pam_profile_path'/system-auth; do if grep -Pq '^h*passwordh+()h+pam_unix.soh+([^# r]+h+)?(sha512|yescrypt)b' '$l_authselect_file'; then echo '- A strong password hashing algorithm is correctly set'

elif grep -Pq '^h*passwordh+()h+pam_unix.soh+([^# r]+h+)?(md5|bigcrypt|sha256|blowfish)b' '$l_authselect_file'; then echo '- A weak password hashing algorithm is set, updating to 'sha512''

sed -ri 's/(^s*passwords+(requisite|required|sufficient)s+pam_unix.sos+.*)(md5|bigcrypt|sha256|blowfish)(s*.*)$/14 sha512/g' '$l_authselect_file'

else echo 'No password hashing algorithm is set, updating to 'sha512''

sed -ri 's/(^s*passwords+(requisite|required|sufficient)s+pam_unix.sos+.*)$/& sha512/g' '$l_authselect_file'

fi done }

Run the following command to update the password-auth and system-auth files in /etc/pam.d to include pam_unix.so with a strong password hashing algorithm argument:

authselect apply-changes

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-171	3.13.16
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
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)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - Ensure at least one file named /etc/pam.d/system-auth exists and matches pattern
Compliant file(s):
      /etc/pam.d/system-auth - regex '(?i)^\h*password\h+(requisite|required|sufficient)\h+pam_unix
\.so(\h+[^#\n\r]+)?\h+(sha512|yescrypt)\b' found - expect '(?i)^\h*password\h+(requisite|required|
sufficient)\h+pam_unix\.so(\h+[^#\n\r]+)?\h+(sha512|yescrypt)\b' found in the following lines:
          22: password    sufficient                                    pam_unix.so sha512 shadow
 try_first_pass use_authtok remember=5

-------------------------
PASSED - Ensure at least one file named /etc/pam.d/password-auth exists and matches pattern
Compliant file(s):
      /etc/pam.d/password-auth - regex '(?i)^\h*password\h+(requisite|required|sufficient)\h
+pam_unix\.so(\h+[^#\n\r]+)?\h+(sha512|yescrypt)\b' found - expect '(?i)^\h*password\h+(requisite|
required|sufficient)\h+pam_unix\.so(\h+[^#\n\r]+)?\h+(sha512|yescrypt)\b' found in the following
 lines:
          20: password    sufficient                                    pam_unix.so sha512 shadow
 try_first_pass use_authtok remember=5
```

4.4.3.4.4 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

Rationale:

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

Solution

Run the following script to verify the active authselect profile includes use_authtok on the password stack's pam_unix.so module lines:

#!/usr/bin/env bash

{ l_pam_profile='$(head -1 /etc/authselect/authselect.conf)'

if grep -Pq -- '^custom/' <<< '$l_pam_profile'; then l_pam_profile_path='/etc/authselect/$l_pam_profile'

else l_pam_profile_path='/usr/share/authselect/default/$l_pam_profile'

fi grep -P -- '^h*passwordh+(requisite|required|sufficient)h+pam_unix.soh+([^# r]+h+)?use_authtokb' '$l_pam_profile_path'/{password,system}-auth }

Example output:

/etc/authselect/custom/custom-profile/password-auth:password sufficient pam_unix.so sha512 shadow {if not 'without-nullok':nullok} use_authtok

/etc/authselect/custom/custom-profile/system-auth:password sufficient pam_unix.so sha512 shadow {if not 'without-nullok':nullok} use_authtok

- IF - the output does not include use_authtok, run the following script:

#!/usr/bin/env bash

{ l_pam_profile='$(head -1 /etc/authselect/authselect.conf)'

if grep -Pq -- '^custom/' <<< '$l_pam_profile'; then l_pam_profile_path='/etc/authselect/$l_pam_profile'

else l_pam_profile_path='/usr/share/authselect/default/$l_pam_profile'

fi for l_authselect_file in '$l_pam_profile_path'/password-auth '$l_pam_profile_path'/system-auth; do if grep -Pq '^h*passwordh+([^# r]+)h+pam_unix.soh+([^# r]+h+)?use_authtokb' '$l_authselect_file'; then echo '- 'use_authtok' is already set'

else echo '- 'use_authtok' is not set. Updating template'

sed -ri 's/(^s*passwords+(requisite|required|sufficient)s+pam_unix.sos+.*)$/& use_authtok/g' '$l_authselect_file'

fi done }

Run the following command to update the password-auth and system-auth files in /etc/pam.d to include the use_authtok argument on the password stack's pam_unix.so lines:

authselect apply-changes

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-171	3.13.16
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
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)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

------------------------
PASSED - Ensure at least one file named /etc/pam.d/system-auth exists and matches pattern
Compliant file(s):
      /etc/pam.d/system-auth - regex '(?i)^\h*password\h+(requisite|required|sufficient)\h+pam_unix
\.so(\h+[^#\n\r]+)?\h+use_authtok\b' found - expect '(?i)^\h*password\h+(requisite|required|
sufficient)\h+pam_unix\.so(\h+[^#\n\r]+)?\h+use_authtok\b' found in the following lines:
          22: password    sufficient                                    pam_unix.so sha512 shadow
 try_first_pass use_authtok remember=5

------------------------
PASSED - Ensure at least one file named /etc/pam.d/password-auth exists and matches pattern
Compliant file(s):
      /etc/pam.d/password-auth - regex '(?i)^\h*password\h+(requisite|required|sufficient)\h
+pam_unix\.so(\h+[^#\n\r]+)?\h+use_authtok\b' found - expect '(?i)^\h*password\h+(requisite|
required|sufficient)\h+pam_unix\.so(\h+[^#\n\r]+)?\h+use_authtok\b' found in the following lines:
          20: password    sufficient                                    pam_unix.so sha512 shadow
 try_first_pass use_authtok remember=5
```

4.5.1.1 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.

Rationale:

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

Note: If yescrypt becomes available in a future release, this would also be acceptable. It is highly recommended that the chosen hashing algorithm is consistent across /etc/libuser.conf, /etc/login.defs, /etc/pam.d/password-auth, and /etc/pam.d/system-auth.

Set password hashing algorithm to sha512.

Edit /etc/libuser.conf and edit or add the following line:

crypt_style = sha512

Edit /etc/login.defs and edit or add the following line:

ENCRYPT_METHOD SHA512

Note: This only effects local users and passwords created after updating the files 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.

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-171	3.13.16
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
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)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - Ensure at least one file named /etc/login.defs exists and matches pattern
Compliant file(s):
      /etc/login.defs - regex '(?i)^\h*ENCRYPT_METHOD\h+SHA512\b' found - expect '(?i)^
\h*ENCRYPT_METHOD\h+SHA512\b' found in the following lines:
          71: ENCRYPT_METHOD SHA512

-------------------------
PASSED - Ensure at least one file named /etc/libuser.conf exists and matches pattern
```

```
Compliant file(s):
      /etc/libuser.conf - regex '(?i)^\h*crypt_style\h*=\h*(sha512|yescrypt)\b' found - expect '(?
i)^\h*crypt_style\h*=\h*(sha512|yescrypt)\b' found in the following lines:
          20: crypt_style = sha512
```

4.5.1.2 Ensure password expiration is 365 days or less

Info

The PASS_MAX_DAYS parameter in /etc/login.defs allows an administrator to force passwords to expire once they reach a defined age. It is recommended that the PASS_MAX_DAYS parameter be set to less than or equal to 365 days.

Rationale:

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.

Impact:

The password expiration must be greater than the minimum days between password changes or users will be unable to change their password

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>

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	CM-1
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	ID.GV-1
CSF	ID.GV-3
CSF	PR.DS-7
CSF	PR.IP-1
CSF	PR.IP-2
CSF	PR.IP-3
CSF	PR.PT-3
GDPR	32.1.b
GDPR	32.4
HIPAA	164.306(a)(1)
ITSG-33	CM-1
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	M1.2.2
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	GS8b
NIAV2	SS3
NIAV2	SS15a
NIAV2	SS16
NIAV2	VL2
NIAV2	VL7a
NIAV2	VL7b
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
QCSC-V1	7.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - users
The command '/bin/awk -F: '$1 !~ /#/ && $2 ~ /^[^!*]*$/ && ($5 == "" || $5 > 365) {print $1":"$5}' /
etc/shadow | /bin/awk '{ print } END { if (NR == 0) print "pass" }'' returned :

awk: fatal: cannot open file `/etc/shadow' for reading (Permission denied)
pass

-------------------------
PASSED - login.defs
Compliant file(s):
      /etc/login.defs - regex '(?i)^[\s]*PASS_MAX_DAYS[\s]' found - expect '(?
i)^[\s]*PASS_MAX_DAYS[\s]+365[\s]*$' found in the following lines:
          25: PASS_MAX_DAYS 365
```

4.5.1.3 Ensure password expiration warning days is 7 or more

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. It is recommended that the PASS_WARN_AGE parameter be set to 7 or more days.

Rationale:

Providing an advance warning that a password will be expiring gives users time to think of a secure password. Users caught unaware may choose a simple password or write it down where it may be discovered.

Solution

Set the PASS_WARN_AGE parameter to 7 in /etc/login.defs :

PASS_WARN_AGE 7

Modify user parameters for all users with a password set to match:

chage --warndays 7 <user>

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	CM-1
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	ID.GV-1
CSF	ID.GV-3
CSF	PR.DS-7
CSF	PR.IP-1
CSF	PR.IP-2
CSF	PR.IP-3
CSF	PR.PT-3
GDPR	32.1.b
GDPR	32.4
HIPAA	164.306(a)(1)
ITSG-33	CM-1
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	M1.2.2
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	GS8b
NIAV2	SS3
NIAV2	SS15a
NIAV2	SS16
NIAV2	VL2
NIAV2	VL7a
NIAV2	VL7b
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
QCSC-V1	7.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - login.defs
Compliant file(s):
      /etc/login.defs - regex '(?i)^[\s]*PASS_WARN_AGE[\s]+' found - expect '(?
i)^[\s]*PASS_WARN_AGE[\s]+7[\s]*$' found in the following lines:
          28: PASS_WARN_AGE 7

-------------------------
PASSED - users
The command '/bin/awk -F: '$1 !~ /#/ && $2 ~ /^[^!*]*$/ && ($6 == "" || $6 < 7) {print $1":"$6}' /
etc/shadow | /bin/awk '{ print } END { if (NR == 0) print "pass" }'' returned :

awk: fatal: cannot open file `/etc/shadow' for reading (Permission denied)
pass
```

4.5.1.5 Ensure all users last password change date is in the past

Info

All users should have a password change date in the past.

Rationale:

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/15289

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

awk: fatal: cannot open file `/etc/shadow' for reading (Permission denied)
Pass
```

4.5.2.1 Ensure default group for the root account is GID 0

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.

Rationale:

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 default group ID to 0:

usermod -g 0 root

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	CM-1
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	5.1
CSCV8	4.1
CSF	DE.AE-1
CSF	ID.GV-1
CSF	ID.GV-3
CSF	PR.DS-7
CSF	PR.IP-1
CSF	PR.IP-2
CSF	PR.IP-3
CSF	PR.PT-3
GDPR	32.1.b
GDPR	32.4
HIPAA	164.306(a)(1)
ITSG-33	CM-1
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	M1.2.2
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	GS8b
NIAV2	SS3
NIAV2	SS15a

NIAV2	SS16
NIAV2	VL2
NIAV2	VL7a
NIAV2	VL7b
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
QCSC-V1	7.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: ^root:x:0:0:

file: /etc/passwd regex: ^root:

Hosts

10.74.6.135

```
Compliant file(s):
      /etc/passwd - regex '^root:' found - expect '^root:x:0:0:' found in the following lines:
          1: root:x:0:0:root:/root:/bin/bash
```

4.5.2.3 Ensure system accounts are secured

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.

Rationale:

It is important to make sure that accounts that are not being used by regular users are prevented from being used to provide an interactive shell. By default, most distributions set the password field for these accounts to an invalid string, but it is also recommended that the shell field in the password file be set to the nologin shell. This prevents the account from potentially being used to run any commands.

Solution

System accounts

Set the shell for any accounts returned by the audit to nologin:

usermod -s $(command -v nologin) <user>

Disabled accounts

Lock any non root accounts returned by the audit:

usermod -L <user>

Large scale changes

The following command will set all system accounts to nologin:

awk -F: '($1!~/^(root|halt|sync|shutdown|nfsnobody)$/ && ($3<"$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)" || $3 == 65534)) { print $1 }' /etc/passwd | while read user; do usermod -s $(command -v nologin) $user >/dev/null; done

The following command will automatically lock all accounts that have their shell set to nologin:

awk -F: '/nologin/ {print $1}' /etc/passwd | while read user; do usermod -L $user; done

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
PASSED - nologin
The command '/bin/awk -F: '($1!~/^(root|halt|sync|shutdown|nfsnobody)$/ && ($3<'"$(awk '/^
\s*UID_MIN/{print $2}' /etc/login.defs)"' || $3 == 65534) && $7!~/^(\/usr)?\/sbin\/nologin$/)
 { print $1 }' /etc/passwd | /bin/awk '{print} END {if (NR == 0) print "pass" ; else print "fail"}''
 returned :

pass

-------------------------
PASSED - Disabled accounts
```

```
The command '/bin/awk -F: '/nologin/ {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' | awk
 '($2!="L" && $2!="LK") {print $1}' | /bin/awk '{print} END {if (NR == 0) print "pass" ; else print
 "fail"}'' returned :

Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root can do that.
Only root ca [...]
```

4.5.3.2 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 the .bash_profile, however this file is used to set an initial PATH or PS1 for all shell users of the system. is only executed for interactive login shells, or shells executed with the --login parameter.

/etc/profile.d - /etc/profile will execute the scripts within /etc/profile.d/*.sh. It is recommended to place your configuration in a shell script within /etc/profile.d to set your own system wide environmental variables.

/etc/bashrc - System wide version of .bashrc. In Fedora derived distributions, /etc/bashrc also invokes /etc/profile.d/*.sh if non-login shell, but redirects output to /dev/null if non-interactive. Is only executed for interactive shells or if BASH_ENV is set to /etc/bashrc.

Rationale:

Setting a timeout value reduces the window of opportunity for unauthorized user access to another user's shell session that has been left unattended. It also ends the inactive session and releases the resources associated with that session.

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 in .sh

/etc/profile

/etc/bashrc

TMOUT configuration examples:

As multiple lines:

TMOUT=900 readonly TMOUT export TMOUT

As a single line:

readonly TMOUT=900 ; export TMOUT

Additional Information:

The audit and remediation in this recommendation apply to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked. Other methods of setting a timeout exist for other shells not covered here.

Ensure that the timeout conforms to your local policy.

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.1
800-171	3.1.10
800-171	3.1.11
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(a)(2)(iii)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*passed:?[\s]***$

Hosts

10.74.6.135

```
The command script with multiple lines returned :

PASSED

TMOUT is configured in: "/etc/profile.d/tmout.sh"
```

4.5.3.3 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 or .bashrc), in their home directory.

Setting the default umask:

pam_umask module:

will set the umask according to the system default in /etc/login.defs and user settings, solving the problem of different umask settings with different shells, display managers, remote sessions etc.

umask=<mask> value in the /etc/login.defs file is interpreted as Octal

Setting USERGROUPS_ENAB to yes in /etc/login.defs (default):

will enable setting of the umask group bits to be the same as owner bits. (examples: 022 -> 002, 077 -> 007) for non-root users, if the uid is the same as gid, and username is the same as the <primary group name>

userdel will remove the user's group if it contains no more members, and useradd will create by default a group with the name of the user

System Wide Shell Configuration File:

/etc/profile - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in the .bash_profile, however this file is used to set an initial PATH or PS1 for all shell users of the system. is only executed for interactive login shells, or shells executed with the --login parameter.

/etc/profile.d - /etc/profile will execute the scripts within /etc/profile.d/*.sh. It is recommended to place your configuration in a shell script within /etc/profile.d to set your own system wide environmental variables.

/etc/bashrc - System wide version of .bashrc. In Fedora derived distributions, etc/bashrc also invokes /etc/profile.d/*.sh if non-login shell, but redirects output to /dev/null if non-interactive. Is only executed for interactive shells or if BASH_ENV is set to /etc/bashrc.

User Shell Configuration Files:

~/.bash_profile - Is executed to configure your shell before the initial command prompt. Is only read by login shells.

~/.bashrc - Is executed for interactive shells. only read by a shell that's both interactive and non-login

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 in .sh - 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

Rationale:

Setting a secure default value for umask ensures that users make a conscious choice about their file permissions. A permissive umask value could result in directories or files with excessive permissions that can be read and/or written to by unauthorized users.

Solution

Run the following script and perform the instructions in the output:

#!/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 }

Note:

This method only applies to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked

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

Default Value:

UMASK 022

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$ timeout: 7200

Hosts

10.74.6.135

```
The command script with multiple lines returned :

- Audit Result:
  ** PASS **
 - * Correctly configured * :

 - umask is set correctly in "/etc/profile"
 - umask is set correctly in "/etc/bashrc"
 - umask is set correctly in "/etc/login.defs"
```

5.1.1.1 Ensure rsyslog is installed

Info

The rsyslog software is recommended in environments where journald does not meet operation requirements.

Rationale:

The security enhancements of rsyslog such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server) justify installing and configuring the package.

Solution

Run the following command to install rsyslog:

dnf install rsyslog

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)

HIPAA	164.312(b)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: gt required: YES rpm: rsyslog-0.0.0-0

Hosts

10.74.6.135

```
The local RPM is newer than rsyslog-0.0.0-0 (rsyslog-8.2102.0-15.el8)
```

5.1.1.2 Ensure rsyslog service is enabled

Info

Once the rsyslog package is installed, ensure that the service is enabled.

Rationale:

If the rsyslog service is not enabled to start on boot, the system will not capture logging events.

Solution

Run the following command to enable rsyslog:

systemctl --now enable rsyslog

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: /bin/systemctl is-enabled rsyslog | /bin/awk '{print} END {if(NR==0) print "disabled" }'

expect: ^enabled$

Hosts

10.74.6.135

```
The command '/bin/systemctl is-enabled rsyslog | /bin/awk '{print} END {if(NR==0) print
 "disabled" }'' returned :

enabled
```

5.1.1.3 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.

Rationale:

-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

Create or edit the file /etc/systemd/journald.conf, or a file in the /etc/systemd/journald.conf.d/ directory ending in .conf and add or edit the line ForwardToSyslog=yes:

Example:

printf '%s ' 'ForwardToSyslog=yes' > /etc/systemd/journald.conf.d/50-journald_forward.conf

Restart the systemd-journald service:

systemctl restart systemd-journald.service

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.5
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-2
ITSG-33	AU-6(3)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1M
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
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 - ForwardToSyslog
The command script with multiple lines returned :

- Audit Result:
  ** PASS **

 - "ForwardToSyslog" is correctly set to "yes" in "/etc/systemd/journald.conf"

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

5.1.1.4 Ensure rsyslog default file permissions are configured

Info

RSyslog will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

Rationale:

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Impact:

The systems global umask could override, but only making the file permissions stricter, what is configured in RSyslog with the FileCreateMode directive. RSyslog also has its own $umask directive that can alter the intended file creation mode. In addition, consideration should be given to how FileCreateMode is used.

Thus it is critical to ensure that the intended file creation mode is not overridden with less restrictive settings in /etc/rsyslog.conf, /etc/rsyslog.d/*conf files and that FileCreateMode is set before any file is created.

Solution

Edit either /etc/rsyslog.conf or a dedicated .conf file in /etc/rsyslog.d/ and set $FileCreateMode to 0640 or more restrictive:

$FileCreateMode 0640

Restart the service:

systemctl restart rsyslog

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

expect: \$FileCreateMode 0[0246][024]0[\s]*$ file: /etc/rsyslog.conf /etc/rsyslog.d/*.conf min_occurrences: 1 regex: ^[\s]*\$FileCreateMode string_required: NO

Hosts

10.74.6.135

```
Compliant file(s):
      /etc/rsyslog.conf - regex '^[\s]*\$FileCreateMode' found - expect '\$FileCreateMode 0[0246]
[024]0[\s]*$' found in the following lines:
          156: $FileCreateMode 0640
      /etc/rsyslog.d/siem.conf - regex not found
```

5.1.1.6 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.

Rationale:

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

Solution

Edit the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files 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.

. action(type='omfwd' target='192.168.2.100' port='514' protocol='tcp'

action.resumeRetryCount='100'

queue.type='LinkedList' queue.size='1000')

Run the following command to reload the rsyslogd configuration:

systemctl restart rsyslog

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
FAILED - rsyslog new format
```

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

------------------------
PASSED - rsyslog old format
Compliant file(s):
      /etc/rsyslog.conf - regex '^\s*[^#]+\.\*\s+@' found - expect '^\s*[^#]+\.\*\s+@' found in the
 following lines:
          154: *.* @@10.74.2.55:514
          159: *.* @@logagg.example.com
      /etc/rsyslog.d/siem.conf - regex '^\s*[^#]+\.\*\s+@' found - expect '^\s*[^#]+\.\*\s+@' found
 in the following lines:
          2: *.*  @10.74.2.55:514
```

5.1.1.7 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.

Rationale:

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

Should there be any active log server configuration found in the auditing section, modify those files and remove the specific lines highlighted by the audit. Ensure none of the following entries are present in any of /etc/rsyslog.conf or /etc/rsyslog.d/*.conf.

New format

module(load='imtcp') input(type='imtcp' port='514')

-OR- Old format

$ModLoad imtcp $InputTCPServerRun

Restart the service:

systemctl restart rsyslog

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-53	AU-2
800-53	AU-7
800-53	AU-12
800-53	CM-6
800-53	CM-7
800-53R5	AU-2

800-53R5	AU-7
800-53R5	AU-12
800-53R5	CM-6
800-53R5	CM-7
CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(a)
CSCV7	6.2
CSCV7	6.3
CSCV7	9.2
CSCV8	4.8
CSCV8	8.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.IP-1
CSF	PR.PT-1
CSF	PR.PT-3
CSF	RS.AN-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-2
ITSG-33	AU-7
ITSG-33	AU-12
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NESA	M1.2.2
NESA	M5.5.1
NIAV2	AM7
NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	SS15a
NIAV2	SS30
NIAV2	VL8
PCI-DSSV3.2.1	2.2.2
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	2.3
SWIFT-CSCV1	6.4

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

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

-------------------------
WARNING - Manual Review Required - Old format ModLoad imtcp
No matching files were found

-------------------------
WARNING - Manual Review Required - Old format InputTCPServerRun
No matching files were found

-------------------------
WARNING - Manual Review Required - New format input imtcp
No matching files were found

-------------------------
WARNING - Manual Review Required - New format module load imtcp
No matching files were found
```

5.1.2.1.1 Ensure systemd-journal-remote is installed

Info

Journald (via 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.

Rationale:

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

Solution

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

dnf install systemd-journal-remote

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)

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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

5.1.2.1.2 Ensure systemd-journal-remote is configured

Info

Journald (via 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.

Rationale:

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

Solution

Edit the /etc/systemd/journal-upload.conf file and ensure the following lines are set per your environment:

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

Restart the service:

systemctl restart systemd-journal-upload

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

5.1.2.1.3 Ensure systemd-journal-remote is enabled

Info

Journald (via 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.

Rationale:

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

Solution

Run the following command to enable systemd-journal-remote:

systemctl --now enable systemd-journal-upload.service

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)

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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

5.1.2.1.4 Ensure journald is not configured to receive logs from a remote client

Info

Journald 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.

Rationale:

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.

Solution

Run the following command to disable systemd-journal-remote.socket:

systemctl --now mask systemd-journal-remote.socket

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-53	AU-2
800-53	AU-7
800-53	AU-12
800-53	CM-6
800-53	CM-7
800-53R5	AU-2
800-53R5	AU-7
800-53R5	AU-12
800-53R5	CM-6
800-53R5	CM-7

CN-L3	7.1.2.3(c)
CN-L3	8.1.4.3(a)
CSCV7	6.2
CSCV7	6.3
CSCV7	9.2
CSCV8	4.8
CSCV8	8.2
CSF	DE.CM-1
CSF	DE.CM-3
CSF	DE.CM-7
CSF	PR.IP-1
CSF	PR.PT-1
CSF	PR.PT-3
CSF	RS.AN-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-2
ITSG-33	AU-7
ITSG-33	AU-12
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1A
NESA	M1.2.2
NESA	M5.5.1
NIAV2	AM7
NIAV2	AM11a
NIAV2	AM11b
NIAV2	AM11c
NIAV2	AM11d
NIAV2	AM11e
NIAV2	SS15a
NIAV2	SS30
NIAV2	VL8
PCI-DSSV3.2.1	2.2.2
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	2.3

SWIFT-CSCV1 6.4

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

5.1.2.2 Ensure journald service is enabled

Info

Ensure that the systemd-journald service is enabled to allow capturing of logging events.

Rationale:

If the systemd-journald service is not enabled to start on boot, the system will not capture logging events.

Solution

By default the systemd-journald service does not have an [Install] section and thus cannot be enabled / disabled. It is meant to be referenced as Requires or Wants by other unit files. As such, if the status of systemd-journald is not static, investigate why.

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

5.1.2.3 Ensure journald is configured to compress large log files

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.

Rationale:

Uncompressed large files may unexpectedly fill a filesystem leading to resource unavailability. Compressing logs prior to write can prevent sudden, unexpected filesystem impacts.

Solution

Edit the /etc/systemd/journald.conf file and add the following line:

Compress=yes

Restart the service:

systemctl restart systemd-journald.service

Additional Information:

The main configuration file /etc/systemd/journald.conf is read before any of the custom *.conf files. If there are custom configs present, they override the main configuration parameters.

It is possible to change the default threshold of 512 bytes per object before compression is used.

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

5.1.2.4 Ensure journald is configured to write logfiles to persistent disk

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.

Rationale:

Writing log data to disk will provide the ability to forensically reconstruct events which may have impacted the operations or security of a system even after a system crash or reboot.

Solution

Edit the /etc/systemd/journald.conf file and add the following line:

Storage=persistent

Restart the service:

systemctl restart systemd-journald.service

Additional Information:

The main configuration file /etc/systemd/journald.conf is read before any of the custom *.conf files. If there are custom configs present, they override the main configuration parameters.

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

5.1.2.5 Ensure journald is not configured to send logs to rsyslog

Info

Data from journald should be kept in the confines of the service and not forwarded on to other services.

Rationale:

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

Edit the /etc/systemd/journald.conf file and ensure that ForwardToSyslog=yes is removed.

Restart the service:

systemctl restart systemd-journald.service

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.5
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
ITSG-33	AU-2
ITSG-33	AU-6(3)
ITSG-33	AU-7
ITSG-33	AU-12
LEVEL	1M
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

5.1.2.6 Ensure journald log rotation is configured per site policy

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.

Rationale:

By keeping the log files smaller and more manageable, a system administrator can easily archive these files to another system and spend less time looking through inordinately large log files.

Solution

Review /etc/systemd/journald.conf and verify logs are rotated according to site policy. The settings should be carefully understood as there are specific edge cases and prioritization of parameters.

The specific parameters for log rotation are:

SystemMaxUse= SystemKeepFree= RuntimeMaxUse= RuntimeKeepFree= MaxFileSec=

Additional Information:

See man 5 journald.conf for detailed information regarding the parameters in use.

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

5.3.1 Ensure AIDE is installed

Info

Advanced Intrusion Detection Environment (AIDE) is an intrusion detection tool that uses predefined rules to check the integrity of files and directories in the Linux operating system. AIDE has its own database to check the integrity of files and directories.

aide takes a snapshot of files and directories 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.

Rationale:

By monitoring the filesystem state compromised files can be detected to prevent or limit the exposure of accidental or malicious misconfigurations or modified binaries.

Solution

Run the following command to install aide:

dnf install aide

Configure aide as appropriate for your environment. Consult the aide documentation for options.

Initialize aide:

Run the following commands:

aide --init

mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.7
800-171	3.3.1
800-171	3.3.2
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
HIPAA	164.312(b)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

operator: gt required: YES rpm: aide-0.0.0-0

Hosts

10.74.6.135

```
The local RPM is newer than aide-0.0.0-0 (aide-0.16-14.el8_5.1)
```

6.1.1 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.

Rationale:

It is critical to ensure that the /etc/passwd file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

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

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

file: /etc/passwd group: root mask: 133 owner: root

Hosts

10.74.6.135

```
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
```

6.1.2 Ensure permissions on /etc/passwd- are configured

Info

The /etc/passwd- file contains backup user account information.

Rationale:

It is critical to ensure that the /etc/passwd- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

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-

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: { 0/ root)

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

file: /etc/passwd- group: root mask: 133 owner: root

Hosts

10.74.6.135

```
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-
```

6.1.3 Ensure permissions on /etc/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

Rationale:

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

Default Value:

/etc/security/opasswd Access: (0600/-rw-------) Uid: (0/ root) Gid: (0/ root)

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

```
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
The file /etc/security/opasswd.old with fmode owner: root group: root mode: 0600 uid: 0 gid: 0
 uneven permissions : FALSE is compliant with the policy value

/etc/security/opasswd.old
```

6.1.4 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.

Rationale:

The /etc/group file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.

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

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

file: /etc/group group: root mask: 133 owner: root

Hosts

10.74.6.135

```
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
```

6.1.5 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.

Rationale:

It is critical to ensure that the /etc/group- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

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-

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

file: /etc/group- group: root mask: 133 owner: root

Hosts

10.74.6.135

```
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-
```

6.1.6 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.

Rationale:

If attackers can gain read access to the /etc/shadow file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the /etc/shadow file (such as expiration) could also be useful to subvert the user accounts.

Solution

Run the following commands to set mode, owner, and group on /etc/shadow:

chown root:root /etc/shadow # chmod 0000 /etc/shadow

Default Value:

Access: (0/----------) Uid: (0/ root) Gid: (0/ root)

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

file: /etc/shadow group: root mask: 777 owner: root

Hosts

10.74.6.135

```
The file /etc/shadow with fmode owner: root group: root mode: 0000 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/shadow
```

6.1.7 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.

Rationale:

It is critical to ensure that the /etc/shadow- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Solution

Run the following commands to set mode, owner, and group on /etc/shadow-:

chown root:root /etc/shadow- # chmod 0000 /etc/shadow-

Default Value:

Access: (0/----------) Uid: (0/ root) Gid: (0/ root)

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

file: /etc/shadow- group: root mask: 777 owner: root

Hosts

10.74.6.135

```
The file /etc/shadow- with fmode owner: root group: root mode: 0000 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/shadow-
```

6.1.8 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.

Rationale:

If attackers can gain read access to the /etc/gshadow file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the /etc/gshadow file (such as group administrators) could also be useful to subvert the group.

Solution

Run the following commands to set mode, owner, and group on /etc/gshadow:

chown root:root /etc/gshadow # chmod 0000 /etc/gshadow

Default Value:

Access: (0/----------) Uid: (0/ root) Gid: (0/ root)

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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	16.4
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

file: /etc/gshadow group: root mask: 777 owner: root

Hosts

10.74.6.135

```
The file /etc/gshadow with fmode owner: root group: root mode: 0000 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/gshadow
```

6.1.9 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.

Rationale:

It is critical to ensure that the /etc/gshadow- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Solution

Run the following commands to set mode, owner, and group on /etc/gshadow-:

chown root:root /etc/gshadow- # chmod 0000 /etc/gshadow-

Default Value:

Access: (0/----------) Uid: (0/ root) Gid: (0/ root)

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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	16.4
CSCV8	3.3
CSF	PR.AC-4
CSF	PR.DS-5
CSF	PR.PT-2
CSF	PR.PT-3
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

file: /etc/gshadow- group: root mask: 777 owner: root

Hosts

10.74.6.135

```
The file /etc/gshadow- with fmode owner: root group: root mode: 0000 uid: 0 gid: 0 uneven
 permissions : FALSE is compliant with the policy value

/etc/gshadow-
```

6.1.10 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.

Rationale:

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

Default Value:

Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

file: /etc/shells group: root mask: 133 owner: root

Hosts

10.74.6.135

```
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
```

6.1.11 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.

Rationale:

Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.

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_path=(); a_arr=() # Initialize array a_path=(! -path '/run/user/*' -a ! -path '/proc/*' -a ! -path '*/containerd/*' -a ! -path '*/kubelet/pods/*' -a ! -path '/sys/kernel/security/apparmor/*' -a ! -path '/snap/*' -a ! -path '/sys/fs/cgroup/memory/*' -a ! -path '/sys/fs/selinux/*') while read -r l_bfs; do a_path+=(-a ! -path ''$l_bfs'/*') done < <(findmnt -Dkerno fstype,target | awk '$1 ~ /^s*(nfs|proc|smb)/ {print $2}') # Populate array with files while IFS= read -r -d $'0' l_file; do [-e '$l_file'] && a_arr+=('$(stat -Lc '%n^%#a' '$l_file')') done < <(find / ('${a_path[@]}') (-type f -o -type d) -perm -0002 -print0 2>/dev/null) while IFS='^' read -r l_fname l_mode; do # Test files in the array if [-f '$l_fname']; then # Remove excess permissions from WW files echo -e ' - File: '$l_fname' is mode: '$l_mode'

- removing write permission on '$l_fname' from 'other''

chmod o-w '$l_fname'

fi if [-d '$l_fname']; then if [! $(($l_mode & $l_smask)) -gt 0]; then # Add sticky bit echo -e ' - Directory: '$l_fname' is mode: '$l_mode' and doesn't have the sticky bit set

- Adding the sticky bit'
chmod a+t '$l_fname'
fi fi done < <(printf '%s ' '${a_arr[@]}') unset a_path; unset a_arr # Remove array }

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

name: find_world_writeable_files timeout: 7200

Hosts

10.74.6.135

```
No issues found.
```

6.2.1 Ensure accounts in /etc/passwd use shadowed passwords

Info

Local accounts can use 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.

Rationale:

The /etc/passwd file also contains information like user ID's and group ID's that are used by many system programs. Therefore, the /etc/passwd file must remain world readable. In spite of encoding the password with a randomly-generated one-way hash function, an attacker could still break the system if they got access to the /etc/passwd file. This can be mitigated by using shadowed passwords, thus moving the passwords in the /etc/passwd file to /etc/shadow. The /etc/shadow file is set so only root will be able to read and write. This helps mitigate the risk of an attacker gaining access to the encoded passwords with which to perform a dictionary attack.

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:

sed -e 's/^([a-zA-Z0-9_]*):[^:]*:/1:x:/' -i /etc/passwd

Investigate to determine if the account is logged in and what it is being used for, to determine if it needs to be forced off.

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.5.2
800-171	3.13.16
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
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)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: /bin/awk -F: '($2 != "x") { print $1 " is not set to shadowed passwords "}' /etc/passwd | /bin/awk '{print} END {if (NR == 0) print "none"}'

expect: ^none$

Hosts

10.74.6.135

```
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
```

6.2.2 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.

Rationale:

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/15289

References

800-171	3.5.2
800-53	IA-5(1)
800-53R5	IA-5(1)
CSCV7	4.4
CSCV8	5.2
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-5(1)
LEVEL	1A
NESA	T5.2.3
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	4.1

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: /bin/awk -F : '($2 == "") { print $1 " does not have a password."}' /etc/shadow | /bin/awk '{print} END {if (NR == 0) print "none"}'

expect: ^none$

Hosts

10.74.6.135

```
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 :

awk: fatal: cannot open file `/etc/shadow' for reading (Permission denied)
none
```

6.2.3 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 .

Rationale:

Groups defined in the /etc/passwd file but not in the /etc/group file pose a threat to system security since group permissions are not properly managed.

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/15289

References

800-171	3.1.1
800-53	AC-2c.
800-53R5	AC-2c.
CN-L3	7.1.3.2(d)
CSF	DE.CM-1
CSF	DE.CM-3
CSF	PR.AC-1
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
ISO/IEC-27001	A.9.2.1
ITSG-33	AC-2c.
LEVEL	1A
NESA	T5.2.1
NESA	T5.2.2
NIAV2	AM28
NIAV2	NS5j
NIAV2	SS14e
PCI-DSSV3.2.1	1.1.5
PCI-DSSV3.2.1	7.1.1
PCI-DSSV3.2.1	7.1.3
PCI-DSSV4.0	7.2.1

PCI-DSSV4.0	7.2.2
QCSC-V1	5.2.2
QCSC-V1	8.2.1
QCSC-V1	13.2
QCSC-V1	15.2

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

name: passwd_invalid_gid

Hosts

10.74.6.135

```
No issues found.
```

6.2.4 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.

Rationale:

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/15289

References

800-171	3.5.5
800-171	3.5.6
800-53	IA-4d.
800-53R5	IA-4d.
CN-L3	8.1.4.1(a)
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-4d.
LEVEL	1A
NESA	T5.5.2
NIAV2	AM14a
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	5

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

name: passwd_duplicate_uid

Hosts

10.74.6.135

```
No duplicate User IDs detected
```

6.2.5 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.

Rationale:

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/15289

References

800-171	3.5.5
800-171	3.5.6
800-53	IA-4d.
800-53R5	IA-4d.
CN-L3	8.1.4.1(a)
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-4d.
LEVEL	1A
NESA	T5.5.2
NIAV2	AM14a
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	5

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

name: group_duplicate_gid

Hosts

10.74.6.135

```
No duplicate Group IDs detected
```

6.2.6 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 username.

Rationale:

If a user is assigned a duplicate user name, it will create and have access to files with the first UID for that username in /etc/passwd . For example, if 'test4' has a UID of 1000 and a subsequent 'test4' entry has a UID of 2000, logging in as 'test4' will use UID 1000. Effectively, the UID is shared, which is a security problem.

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/15289

References

800-171	3.5.5
800-171	3.5.6
800-53	IA-4d.
800-53R5	IA-4d.
CN-L3	8.1.4.1(a)
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-4d.
LEVEL	1A
NESA	T5.5.2
NIAV2	AM14a
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	5

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

name: passwd_duplicate_username

Hosts

10.74.6.135

```
No issues found.
```

6.2.7 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.

Rationale:

If a group is assigned a duplicate group name, it will create and have access to files with the first GID for that group in /etc/group . Effectively, the GID is shared, which is a security problem.

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/15289

References

800-171	3.5.5
800-171	3.5.6
800-53	IA-4d.
800-53R5	IA-4d.
CN-L3	8.1.4.1(a)
CSF	PR.AC-1
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(2)(i)
HIPAA	164.312(d)
ITSG-33	IA-4d.
LEVEL	1A
NESA	T5.5.2
NIAV2	AM14a
QCSC-V1	5.2.2
QCSC-V1	13.2
SWIFT-CSCV1	5

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

name: group_duplicate_name

Hosts

10.74.6.135

```
No issues found.
```

6.2.9 Ensure root is the only UID 0 account

Info

Any account with UID 0 has superuser privileges on the system.

Rationale:

This access must be limited to only the default root account and only from the system console. Administrative access must be through an unprivileged account using an approved mechanism as noted in Item 5.6 Ensure access to the su command is restricted.

Solution

Remove any users other than root with UID 0 or assign them a new UID if appropriate.

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.5
800-53	AC-6(5)
800-53R5	AC-6(5)
CN-L3	8.1.10.6(a)
CSF	PR.AC-4
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

name: passwd_zero_uid

Hosts

10.74.6.135

```
No issues found.
```

6.2.10 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.

Rationale:

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$

Hosts

10.74.6.135

```
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
```

6.2.11 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 last 500 commands.

Rationale:

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

list .forward and .rhost files to be investigated and manually deleted

#!/usr/bin/env bash

{ 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 [[-n '$l_epu' && -n '$l_eph']] && a_uarr+=('$l_epu $l_eph') done <<< '$(awk -v pat='$l_valid_shells' -F: '$(NF) ~ pat { print $1 ' ' $(NF-1) }' /etc/passwd)'

l_asize='${#a_uarr[@]}' # Here if we want to look at number of users before proceeding l_maxsize='1000' # Maximum number of local interactive users before warning (Default 1,000) ['$l_asize ' -gt '$l_maxsize'] && echo -e '

** INFO **

- '$l_asize' Local interactive users found on the system

- This may be a long running check '

file_access_fix() { l_facout2=''

l_max='$(printf '%o' $((0777 & ~$l_mask)))'

```
if [ $(( $l_mode & $l_mask )) -gt 0 ]; then echo -e ' - File: '$l_hdfile' is mode: '$l_mode' and should be mode: '$l_max' or more restrictive

- Changing to mode '$l_max''

chmod '$l_chp' '$l_hdfile'

fi if [[ ! '$l_owner' =~ ($l_user) ]]; then echo -e ' - File: '$l_hdfile' owned by: '$l_owner' and should be owned by '${l_user//|/ or }'

- Changing ownership to '$l_user''

chown '$l_user' '$l_hdfile'

fi if [[ ! '$l_gowner' =~ ($l_group) ]]; then echo -e ' - File: '$l_hdfile' group owned by: '$l_gowner' and should be group owned by '${l_group//|/ or }'

- Changing group ownership to '$l_group''

chgrp '$l_group' '$l_hdfile'

fi } while read -r l_user l_home; do if [ -d '$l_home' ]; then echo -e '

- Checking user: '$l_user' home directory: '$l_home''

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 '$l_hdfile')' in .forward | .rhost ) echo -e ' - File: '$l_hdfile' exists

- Please investigate and manually delete '$l_hdfile''

;;

.netrc ) l_mask='0177'

l_chp='u-x,go-rwx'

file_access_fix ;;

.bash_history ) l_mask='0177'

l_chp='u-x,go-rwx'

file_access_fix ;;

* ) l_mask='0133'

l_chp='u-x,go-wx'

file_access_fix ;;

esac done <<< '$(stat -Lc '%#a %U %G' '$l_hdfile')'

done < <(find '$l_home' -xdev -type f -name '.*' -print0) fi done <<< '$(printf '%s ' '${a_uarr[@]}')'

unset a_uarr # Remove array }
```

See Also

https://workbench.cisecurity.org/benchmarks/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: multiple line script dont_echo_cmd: NO expect: (?i)^[\s]***[\s]*pass:?[\s]***$ timeout: 7200

Hosts

10.74.6.135

```
The command script with multiple lines returned :

find: '/root': Permission denied
find: '/home/qinstall': Permission denied
find: '/home/juhapkoh': Permission denied
find: '/home/anttimar': Permission denied
find: '/home/jonilouh': Permission denied
find: '/home/insight': Permission denied
find: '/home/karrihav': Permission denied
find: '/home/roberves': Permission denied
find: '/home/juhapell': Permission denied
find: '/opt/nagios': Permission denied
```

```
find: '/opt/consul': Permission denied
find: '/home/jaripehk': Permission denied
find: '/home/viljviit': Permission denied
find: '/home/markarol': Permission denied
find: '/home/pettsaha': Permission denied
find: '/usr/share/logstash': Permission denied
find: '/home/razaisla': Permission denied

- 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
```

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit from CIS Oracle Linux 8 Benchmark v3.0.0

See Also

https://workbench.cisecurity.org/benchmarks/15289

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

PASSED

Hosts

10.74.6.135

Compliance 'INFO', 'WARNING', 'ERROR'

1.2.1 Ensure GPG keys are configured

Info

The RPM Package Manager implements GPG key signing to verify package integrity during and after installation.

Rationale:

It is important to ensure that updates are obtained from a valid source to protect against spoofing that could lead to the inadvertent installation of malware on the system. To this end, verify that GPG keys are configured correctly for your 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/15289

References

800-171	3.11.2
800-171	3.11.3
800-171	3.14.1
800-53	RA-5
800-53	SI-2
800-53	SI-2(2)
800-53R5	RA-5
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
GDPR	32.1.b
GDPR	32.1.d
HIPAA	164.306(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: rpm -q gpg-pubkey --queryformat '%{name}-%{version}-%{release} --> %{summary} '
expect: ^Manual Review Required$

Hosts

10.74.6.135

```
The command 'rpm -q gpg-pubkey --queryformat '%{name}-%{version}-%{release} --> %{summary}\n''
 returned :

gpg-pubkey-81b961a5-64106f70 --> gpg(ELevate <packager@almalinux.org>)
gpg-pubkey-ad986da3-5cabf60d --> gpg(Oracle OSS group (Open Source Software group)
 <build@oss.oracle.com>)
gpg-pubkey-f4a80eb5-53a7ff4b --> gpg(CentOS-7 Key (CentOS 7 Official Signing Key)
 <security@centos.org>)
gpg-pubkey-352c64e5-52ae6884 --> gpg(Fedora EPEL (7) <epel@fedoraproject.org>)
```

1.2.4 Ensure package manager repositories are configured

Info

Systems need to have the respective package manager repositories configured to ensure that the system is able to receive the latest patches and updates.

Rationale:

If a system's package repositories are misconfigured, important patches may not be identified or a rogue repository could introduce compromised software.

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/15289

References

800-171	3.11.2
800-171	3.11.3
800-171	3.14.1
800-53	RA-5
800-53	SI-2
800-53	SI-2(2)
800-53R5	RA-5
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
GDPR	32.1.b
GDPR	32.1.d
HIPAA	164.306(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: /bin/dnf repolist expect: ^Manual Review Required$

Hosts

10.74.6.135

```
The command '/bin/dnf repolist' returned :

No repositories available
```

2.2.22 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.

Rationale:

Services listening on the system pose a potential risk as an attack vector. These services should be reviewed, and if not required, the service should be stopped, and the package containing the service should be removed. If required packages have a dependency, the service should be stopped and masked to reduce the attack surface of the system.

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.

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 # dnf remove <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.

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2

800-171	3.4.6
800-171	3.4.7
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1M
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: /sbin/ss -plntu expect: ^Manual Review Required$

Hosts

10.74.6.135

```
The command '/sbin/ss -plntu' returned :

Netid State  Recv-Q Send-Q Local Address:Port  Peer Address:PortProcess
udp   UNCONN 0      0            0.0.0.0:38736      0.0.0.0:*
udp   UNCONN 0      0          127.0.0.1:8125       0.0.0.0:*
udp   UNCONN 0      0          127.0.0.1:323        0.0.0.0:*
udp   UNCONN 0      0              [::1]:323           [::]:*
tcp   LISTEN 0      128          0.0.0.0:22         0.0.0.0:*
tcp   LISTEN 0      100        127.0.0.1:25         0.0.0.0:*
tcp   LISTEN 0      2048       127.0.0.1:8125       0.0.0.0:*
tcp   LISTEN 0      2048         0.0.0.0:19999      0.0.0.0:*
tcp   LISTEN 0      50         127.0.0.1:9600       0.0.0.0:*
tcp   LISTEN 0      128          0.0.0.0:10050      0.0.0.0:*
tcp   LISTEN 0      5            0.0.0.0:5666       0.0.0.0:*
tcp   LISTEN 0      2048            [::]:19999         [::]:*
tcp   LISTEN 0      128             [::]:10050         [::]:*
tcp   LISTEN 0      5               [::]:5666          [::]:*
```

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 trillion3 addresses.

Features of IPv6

Hierarchical addressing and routing infrastructure

Stateful and Stateless configuration

Support for quality of service (QoS)

An ideal protocol for neighboring node interaction

Rationale:

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

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.

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

Default Value:

IPv6 is enabled

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.4.2
800-171	3.4.6
800-171	3.4.7

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
GDPR	32.1.b
HIPAA	164.306(a)(1)
ITSG-33	CM-6
ITSG-33	CM-7
LEVEL	1M
NIAV2	SS15a
PCI-DSSV3.2.1	2.2.2
SWIFT-CSCV1	2.3

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

cmd: /bin/grep -Pqs '^\h*0\b' /sys/module/ipv6/parameters/disable && echo -e "

- IPv6 is enabled " || echo -e "

- IPv6 is not enabled "

expect: Manual Review Required

Hosts

10.74.6.135

```
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 :

- IPv6 is enabled
```

4.2.22 Ensure sshd crypto_policy is not set

Info

System-wide Crypto policy can be over-ridden or opted out of for openSSH

Rationale:

Over-riding or opting out of the system-wide crypto policy could allow for the use of less secure Ciphers, MACs, KexAlgorithms and GSSAPIKexAlgorithm

Note: If changes to the system-wide crypto policy are required to meet local site policy for the openSSH server, these changes should be done with a sub-policy assigned to the system-wide crypto policy. For additional information see the CRYPTO-POLICIES(7) man page

Solution

Run the following commands:

sed -ri 's/^s*(CRYPTO_POLICYs*=.*)$/# 1/' /etc/sysconfig/sshd

systemctl reload sshd

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.1.13
800-171	3.5.2
800-171	3.13.8
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
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/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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Hosts

10.74.6.135

```
File permission denied: /etc/sysconfig/sshd
```

4.3.3 Ensure sudo log file exists

Info

The Defaults logfile entry sets the path to the sudo log file. Setting a path turns on logging to a file; negating this option turns it off. By default, sudo logs via syslog.

Rationale:

Defining a dedicated log file for sudo simplifies auditing of sudo commands and creation of auditd rules for sudo.

Impact:

WARNING: Editing the sudo configuration incorrectly can cause sudo to stop functioning. Always use visudo to modify sudo configuration files.

Creation of additional log files can cause disk space exhaustion if not correctly managed. You should configure logrotate to manage the sudo log in accordance with your local policy.

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:

Defaults logfile='<PATH TO CUSTOM LOG FILE>'

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.

See Also

https://workbench.cisecurity.org/benchmarks/15289

References

800-171	3.3.1
800-171	3.3.2
800-171	3.3.6

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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(b)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Hosts

10.74.6.135

```
File permission denied: /etc/sudoers
```

4.3.5 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.

Rationale:

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

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

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/15289

References

800-171	3.1.5
800-171	3.1.6
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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Hosts

10.74.6.135

```
File permission denied: /etc/sudoers
```

5.1.3 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/syslog is the configuration file used to rotate log files created by syslog or rsyslog.

Rationale:

By keeping the log files smaller and more manageable, a system administrator can easily archive these files to another system and spend less time looking through inordinately large log files.

NOTE: Nessus has not performed this check. Please review the benchmark to ensure target compliance.

Solution

Edit /etc/logrotate.conf and /etc/logrotate.d/* to ensure logs are rotated according to site policy.

See Also

https://workbench.cisecurity.org/benchmarks/15289

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)
ITSG-33	AU-4
LEVEL	1M
NESA	T3.3.1
NESA	T3.6.2
QCSC-V1	8.2.1
QCSC-V1	13.2

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

WARNING

Hosts

10.74.6.135

6.1.13 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.

Rationale:

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/15289

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
800-53	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
GDPR	32.1.b
HIPAA	164.306(a)(1)
HIPAA	164.312(a)(1)
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Policy Value

name: find_suid_sgid_files timeout: 7200

Hosts

10.74.6.135

```
The following 36 files are SUID or SGID:

  /usr/bin/chfn
     owner: root, group: root, permissions: 4711

  /usr/bin/chsh
     owner: root, group: root, permissions: 4711

  /usr/bin/locate
     owner: root, group: slocate, permissions: 2711

  /usr/bin/mount
     owner: root, group: root, permissions: 4755

  /usr/bin/chage
     owner: root, group: root, permissions: 4755

  /usr/bin/gpasswd
     owner: root, group: root, permissions: 4755

  /usr/bin/newgrp
     owner: root, group: root, permissions: 4755

  /usr/bin/su
     owner: root, group: root, permissions: 4755

  /usr/bin/umount
     owner: root, group: root, permissions: 4755

  /usr/bin/write
     owner: root, group: tty, permissions: 2755

  /usr/bin/sudo
```

```
      owner: root, group: root, permissions: 4111

   /usr/bin/crontab
      owner: root, group: root, permissions: 4755

   /usr/bin/pkexec
      owner: root, group: root, permissions: 4755

   /usr/bin/passwd
      owner: root, group: root, permissions: 4755

   /usr/bin/fusermount
      owner: root, group: root, permissions: 4755

   /usr/bin/ksu
      owner: root, group: root, permissions: 4755

   /usr/bin/screen
      owner: root, group: screen, permissions: 2755

   /usr/sbin/pam_timestamp_check
      owner: root, group: root, permissions: 4755

   /usr/sbin/unix_chkpwd
      owner: root, group: root, permissions: 4755

   /usr/sbin/usernetctl
      owner: root, group: root, permissions: 4755

   /usr/sbin/postdrop
      owner: root, group: postdrop, permissions: 2755

   /usr/sbin/postqueue
      owner: root, group: postdrop, permissions: 2755

   /usr/sbin/mount.nfs
      owner: root, group: root, permissions: 4755

   /usr/sbin/grub2-set-bootflag
      owner: root, group: root, permissions: 4755

   /usr/lib/polkit-1/polkit-agent-helper-1
      owner: root, group: root, permissions: 4755

   /usr/libexec/utempter/utempter
      owner: root, group: utmp, permissions: 2711

   /usr/libexec/dbus-1/dbus-daemon-launch-helper
      owner: root, group: dbus, permissions: 4750

   /usr/libexec/openssh/ssh-keysign
      owner: root [...]
```

6.2.8 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.

Rationale:

Including the current working directory (.) or other writable directory in root's executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as root to execute a Trojan horse program.

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/15289

References

800-171	3.4.7
800-53	CM-7(2)
800-53R5	CM-7(2)
CSF	PR.IP-1
CSF	PR.PT-3
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

Audit File

CIS_Oracle_Linux_8_Server_L1_v3.0.0.audit

Hosts

10.74.6.135

```
Executing the command script with multiple lines failed :
ERROR: Command output has been interrupted.
```